



# GDPR Articles With Commentary & EU Case Laws

Author  
Adv. Prashant Mali

# **GDPR Articles With Commentary & EU Case Laws**

**Author**

**Adv. Prashant Mali**

**[M.Sc.(Computer Science), CCFP, CISSA,LLM, Ph.D(Pursu.)]**

**About Author:**

Author is International Cyber Law & Privacy Expert and a practicing High Court Lawyer based out of Mumbai in India. He is Masters in Computer Science and Masters in Law with Certification in Computer Forensics & Information Systems Security Auditing and prior working experience in the field of Software, Networking & IT Security. He is Chevening (UK) Cyber Security Fellow & IVLP (USA). He is the founder president of a law firm named Cyber Law Consulting. He was awarded as Cyber Security Lawyer of the year (Asia Pacific) in 2016 and Cyber Security Lawyer of the Year by Financial Monthly Magazine of UK. He has been a sought after speaker on National and International forums and is interviewed by BBC World, Bloomberg, Zee News, NDTV, CNBC, Al Jazeera etc. His articles are published in various magazines across the world and he is been quoted by leading daily newspapers. He has conducted various workshops on GDPR in various countries and has unique way of explaining GDPR with examples and by comparing it to existing laws of the country.

**Note:**

Every effort has been made to avoid errors or omissions in this, errors may creep in any mistake, error or discrepancy noted may be brought to our notice which shall be taken care of in the next edition. It is notified that neither the publisher or the author or seller will be responsible for any damages or loss of action to any one, of any kind, in the manner, there from. It is suggested that to avoid any doubt the reader should cross-check all the facts, law and contents of the publication with original Government publication or notification.

All rights reserved. No part of this work may be copied, reproduced, adapted, abridged or translated. Stored in any retrieval system, computer system, photographic or other system or transmitted in any form by any means whether electronic, mechanical, digital, optical photographic or otherwise without the prior written permission of cyber Infomedia. Any breach will entail legal action and prosecution without further notice.

## INDEX

Articles	Particular	Page No.
	<b>CHAPTER 1 : GENERAL PROVISIONS</b>	
1	GDPR Subject-matter and objectives	01
2	GDPR Material scope	03
3	GDPR Territorial scope	04
4	GDPR Definitions	10
	<b>CHAPTER 2 : PRINCIPLES</b>	14
5	GDPR Principles relating to processing of personal data	14
6	GDPR Lawfulness of processing	17
7	GDPR Conditions for consent	20
8	GDPR Conditions applicable to child's consent in relation to information society services	23
9	GDPR Processing of special categories of personal data	24
10	GDPR Processing of personal data relating to criminal convictions and offences	28
11	GDPR Processing which does not require identification	29
	<b>CHAPTER 3 : RIGHTS OF THE DATA SUBJECT</b>	30
	<b>Section 1 : Transparency and modalities</b>	
12	GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject	30
	<b>Section 2 : Information and access to personal data</b>	32
13	GDPR Information to be provided where personal data are collected from the data subject	32
14	GDPR Information to be provided where personal data have not been obtained from the data subject	34

15	GDPR Right of access by the data subject	37
	<b>Section 3 : Rectification and erasure</b>	38
16	GDPR Right to rectification	38
17	GDPR Right to erasure ('right to be forgotten')	39
18	GDPR Right to restriction of processing	41
19	GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing	42
20	GDPR Right to data portability	43
	<b>Section 4 : Right to object and automated individual decision-making</b>	44
21	GDPR Right to object	44
22	GDPR Automated individual decision-making, including profiling	46
	<b>Section 5 : Restrictions</b>	47
23	GDPR Restrictions	47
	<b>CHAPTER 4 : CONTROLLER AND PROCESSOR</b>	49
	<b>Section 1 : General obligations</b>	
24	GDPR Responsibility of the controller	49
25	GDPR Data protection by design and by default	52
26	GDPR Joint controllers	55
27	GDPR Representatives of controllers or processors not established in the Union	58
28	GDPR Processor	60
29	GDPR Processing under the authority of the controller or processor	64
30	GDPR Records of processing activities	64
31	GDPR Cooperation with the supervisory authority	67
	<b>Section 2 : Security of personal data</b>	68

32	GDPR Security of processing	68
33	GDPR Notification of a personal data breach to the supervisory authority	72
34	GDPR Communication of a personal data breach to the data subject	74
	<b>Section 3 : Data protection impact assessment and prior consultation</b>	77
35	GDPR Data protection impact assessment	77
36	GDPR Prior consultation	82
	<b>Section 4 : Data protection officer</b>	84
37	GDPR Designation of the data protection officer	84
38	GDPR Position of the data protection officer	86
39	GDPR Tasks of the data protection officer	88
	<b>Section 5 : Codes of conduct and certification</b>	93
40	GDPR Codes of conduct	93
41	GDPR Monitoring of approved codes of conduct	96
42	GDPR Certification	99
43	GDPR Certification bodies	100
	<b>CHAPTER 5 : TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS</b>	104
44	GDPR General principle for transfers	104
45	GDPR Transfers on the basis of an adequacy decision	106
46	GDPR Transfers subject to appropriate safeguards	109
47	GDPR Binding corporate rules	112
48	GDPR Transfers or disclosures not authorised by Union law	116
49	GDPR Derogations for specific situations	117

50	GDPR International cooperation for the protection of personal data	121
	<b>CHAPTER 6 : INDEPENDENT SUPERVISORY AUTHORITIES</b>	123
	<b>Section 1 : Independent status</b>	
51	GDPR Supervisory authority	123
52	GDPR Independence	124
53	GDPR General conditions for the members of the supervisory authority	126
54	GDPR Rules on the establishment of the supervisory authority	127
	<b>Section 2 : Competence, tasks and powers</b>	128
55	GDPR Competence	128
56	GDPR Competence of the lead supervisory authority	129
57	GDPR Tasks	131
58	GDPR Powers	134
59	GDPR Activity reports	137
	<b>CHAPTER 7 : COOPERATION AND CONSISTENCY</b>	138
	<b>Section 1 : Cooperation</b>	
60	GDPR Cooperation between the lead supervisory authority and the other supervisory authorities concerned	138
61	GDPR Mutual assistance	140
62	GDPR Joint operations of supervisory authorities	142
	<b>Section 2 : Consistency</b>	144
63	GDPR Consistency mechanism	144
64	GDPR Opinion of the Board	144
65	GDPR Dispute resolution by the Board	146

66	GDPR Urgency procedure	148
67	GDPR Exchange of information	149
	<b>Section 3 : European data protection board</b>	149
68	GDPR European Data Protection Board	149
69	GDPR Independence	150
70	GDPR Tasks of the Board	150
71	GDPR Reports	154
72	GDPR Procedure	154
73	GDPR Chair	154
74	GDPR Tasks of the Chair	155
75	GDPR Secretariat	155
76	GDPR Confidentiality	157
	<b>CHAPTER 8 : REMEDIES, LIABILITY AND PENALTIES</b>	158
77	GDPR Right to lodge a complaint with a supervisory authority	158
78	GDPR Right to an effective judicial remedy against a supervisory authority	158
79	GDPR Right to an effective judicial remedy against a controller or processor	160
80	GDPR Representation of data subjects	161
81	GDPR Suspension of proceedings	162
82	GDPR Right to compensation and liability	163
83	GDPR General conditions for imposing administrative fines	163
84	GDPR Penalties	170
	<b>CHAPTER 9 : PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS</b>	171



85	GDPR Processing and freedom of expression and information	171
86	GDPR Processing and public access to official documents	171
87	GDPR Processing of the national identification number	171
88	GDPR Processing in the context of employment	172
89	GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	173
90	GDPR Obligations of secrecy	175
91	GDPR Existing data protection rules of churches and religious associations	176
	<b>CHAPTER 10 : DELEGATED ACTS AND IMPLEMENTING ACTS</b>	178
92	GDPR Exercise of the delegation	178
93	GDPR Committee procedure	179
	<b>CHAPTER 11 : FINAL PROVISIONS</b>	181
94	GDPR Repeal of Directive 95/46/EC	181
95	GDPR Relationship with Directive 2002/58/EC	181
96	GDPR Relationship with previously concluded Agreements	182
97	GDPR Commission reports	182
98	GDPR Review of other Union legal acts on data protection	183
99	GDPR Entry into force and application	183
	<b>CASE LAWS</b>	185
	<b>I. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (IN NUMERICAL ORDER OF CASE NUMBER)</b>	186

<b>1</b>	<b>COURT OF JUSTICE DECISIONS</b>	
1.1	C-450/00, COMMISSION V. LUXEMBOURG, 4.10.2001 ("LUXEMBOURG")	186
1.2	C-465/00 AND C-138/01, RECHNUNGSHOF V. OSTERREICHISCHER RUNDFUNK, 20.5.2003 ("RECHNUNGSHOF")	186
1.3	C-101/01, LINDQUIST, 6.11.2003 ("LINDQUIST")	187
1.4	C-317 AND 318/04, PARLIAMENT V. COUNCIL (PNR), 30.5.2006 ("PNR")	189
1.5	C-275/06, PROMUSICAE, 29.1.2008 ("PROMUSICAE")	189
1.6	C-301/06, IRELAND V. PARLIAMENT AND COUNCIL, 10.2.2009 ("IRELAND")	190
1.7	C-524/06, HUBER V. GERMANY, 16.12.2008 ("HUBER")	191
1.8	C-73/07, TIETOSUOJAVALTUUTETTU [FINNISH DATA PROTECTION OMBUDSMAN] V. SATAKUNNAN MARKKINAPORSSI OY AND SATAMEDIA OY, 16.12.2008 ("TIETOSUOJAVALTUUTETTU")	192
1.9	C-518/07, COMMISSION V. GERMANY, 9.3.2010 ("GERMANY")	193
1.10	C-553/07, COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN ROTTERDAM V. RIJKEBOER, 7.5.2009 ("RIJKEBOER")	194
1.11	C-557/07, LSG-GESELLSCHAFT ZUR WAHRNEHMUNG VON LEISTUNGSSCHUTZRECHTEN GMBH V. TELE2 TELECOMMUNICATION GMBH, 19.2.2009 ("LSG")	194
1.12	C-28/08, COMMISSION V. BAVARIAN LAGER CO., 29.6.2010 ("BAVARIAN LAGER")	195
1.13	C-92/09 VOLKER UND MARKUS SCHECKE GBR V. LAND HESSEN, AND C-93/09, EIFERT V. LAND HESSEN AND BUNDESANSTALT FUR LANDWIRTSCHAFT UND ERNAHRUNG, 9.11.2010 ("SCHECKE")	198

1.14	CASE C-70/10, SCARLET EXTENDED SA V. SOCIETE BELGE DES AUTEURS, COMPOSITEURS ET EDITEURS SCRL (SABAM), 24.11.2011 ("SCARLET")	200
1.15	CASE C-461/10, BONNIER AUDIO AB ET AL. V. PERFECT COMMUNICATION SWEDEN, 19.4.2012 ("BONNIER")	201
1.16	JOINED CASES C-468/10 AND C-469/10, ASOCIACION NACIONAL DE ESTABLECIMIENTOS FINANCIEROS DE CREDITO (ASNEF) AND FEDERACION DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECEMD) V. ADMINISTRACION DEL ESTADO, 24.11.2011 ("ASNEF")	202
1.17	C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 ("AUSTRIA")	203
1.18	C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 ("AUSTRIA")	204
1.19	C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE")	205
1.20	C-141/12 AND C-372/12, MINISTER VOOR IMMIGRATIE V. M, 17.7.2014 ("M")	209
1.21	C-288/12, COMMISSION V. HUNGARY, 8.4.2014 ("HUNGARY")	210
1.22	C-291/12, SCHWARZ V. BOCHUM, 17.10.2014 ("SCHWARZ")	210
1.23	C-293/12 AND C-594-12, DIGITAL RIGHTS IRELAND LTD V. IRELAND, 8.4.2014 ("DRI")	211
1.24	C-342-12, WORTEN-EQUIPAMENTOS PARA O LAR SA V. ACT (AUTHORITY FOR WORKING CONDITIONS), 30.5.2013 ("WORTEN")	214
1.25	C-473/12, IPI V. ENGLEBERT ("ENGLEBERT")	215
1.26	C-486/12, X, 12.12.2013 ("X")	216
1.27	C-212/13, RYNES V. ÚŘAD PRO OCHRANU OSOBNICH ÚDAJŮ, 11.12.2014 ("RYNES")	216
1.28	C-615/13 P, CLIENT EARTH ET AL. V. EFSA, 16.7.2015 ("CLIENT EARTH")	217

1.29	C-201/14, SMARANDA BARA ET AL. V. PRESEDINTELE CASEI NATIONALE DE ASIGURARI DE SANATATE (CNAS) ET AL., 1.10.2015 (“BARA”)	219
1.30	C-230/14, WELTIMMO S.R.O. V. NEMZETI ADATVEDELMI ES INFORMACIOSZABADSAG HATOSAG (HUNGARIAN DPA), 1.10.15 (“WELTIMMO”)	220
1.31	C-362/14, SCHREMS V. DATA PROTECTION COMMISSIONER, 6.10.2015 (“SCHREMS”)	222
<b>2</b>	<b>GENERAL COURT DECISIONS</b>	224
2.1	T-320/02, ESCH-LEONHARDT AND OTHERS V EUROPEAN CENTRAL BANK, 18.2.2004 (“ESCH-LEONHARDT”)	224
2.2	T-198/03, BANK AUSTRIA CREDITANSTALT AG V COMMISSION OF THE EUROPEAN COMMUNITIES, 30.5.2006 (“BANK AUSTRIA”)	225
2.3	T-259/03, NIKOLAOU V. COMMISSION, 12.9.2007 (“NIKOLAOU”)	225
2.4	T-161/04, JORDANA V. COMMISSION, 7.7.2011 (“JORDANA”)	227
2.5	T-82/09, DENNEKAMP V. EUROPEAN PARLIAMENT, 23.11.2011 (“DENNEKAMP I”)	227
2.6	T-190/10, EGAN & HACKETT V. EUROPEAN PARLAMENT, 28.3.2012 (“EGAN & HACKETT”)	228
2.7	T-115/13, DENNEKAMP V. EUROPEAN PARLIAMENT (15.7.2015) (“DENNEKAMP II”)	229
2.8	T-496/13, MCCULLOUGH V. CEDEFOP (11.6.2015)(“MCCULLOUGH”)	231
<b>3</b>	<b>CIVIL SERVICE TRIBUNAL DECISIONS</b>	232
3.1	F-30/08, NANOPOULOS V. COMMISSION, 11.5.2010 (“NANOPOULOS”) (ON APPEAL, CASE T-308/10)	232
3.2	F-46/09, V & EDPS V. EUROPEAN PARLAMENT, 5.7.2011 (“V”)	232
<b>4</b>	<b>POST GDPR IMPLEMENTATION CASE LAWS</b>	234
4.1	GOOGLE CASE	234

4.2	GERMAN COURTS - WHETHER AN INFRINGEMENT OF THE GDPR ALSO QUALIFIES AS UNFAIR-COMPETITIVE BEHAVIOR	235
4.3	GOOGLE IN LANDMARK NORDIC LEGAL CASE ON THE “RIGHT TO BE FORGOTTEN.”	236
4.4	GDPR FINE –BARREIRO MONTIJO HOSPITAL CENTER IN PORTUGAL CASE	237
4.5	FACEBOOK BREACH IN GDPR TEST CASE.	238
	<b>II. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (ORGANISED BY TOPIC)</b>	239
<b>1</b>	<b>GENERAL</b>	239
1.1	DEFINITION OF PERSONAL DATA	239
1.2	DEFINITION OF PROCESSING	240
1.3	DEFINITION OF CONTROLLER	241
1.4	LEGAL PERSONS	242
1.5	SENSITIVE PERSONAL DATA	242
1.6	CONSENT	243
1.7	NECESSITY/PROPORTIONALITY	243
1.8	SECURITY	245
1.9	DEROGATIONS	245
1.10	NON-CONTRACTUAL LIABILITY	246
<b>2</b>	<b>DATA SUBJECT RIGHTS</b>	246
2.1	INFORMATION	246
2.2	ACCESS	247
2.3	ERASURE	248
<b>3</b>	<b>BALANCING FUNDAMENTAL RIGHTS</b>	248
3.1	PROTECTION OF PROPERTY AND AN EFFECTIVE REMEDY	248

3.2	FREEDOM OF EXPRESSION	249
3.2	ACCESS TO DOCUMENTS	249
<b>4</b>	<b>TRANSFERS</b>	252
4.1	APPROPRIATE LEGAL BASIS	254
4.2	ADEQUATE LEVEL OF PROTECTION	254
4.3	SAFE HARBOUR	255
<b>5</b>	<b>REGULATION 45/2001</b>	256
5.1	SCOPE	256
5.2	LAWFULNESS	256
<b>6</b>	<b>DIRECTIVE 95/46</b>	256
6.1	SCOPE	256
6.2	LAWFULNESS	257
6.3	ESTABLISHMENT OF THE CONTROLLER	257
6.4	INDEPENDENCE OF DPA	259
6.5	DPA POWERS	261
6.6	PROCESSING FOR SOLELY JOURNALISTIC PURPOSES	262
6.7	PROCESSING FOR PURELY PERSONAL OR HOUSEHOLD ACTIVITY	262
6.8	TRANSPOSITION/HARMONISATION	263
6.9	DIRECT APPLICABILITY	263
<b>7</b>	<b>DIRECTIVE 2002/58</b>	264
7.1	SCOPE	264
7.2	TRAFFIC DATA	264
<b>8</b>	<b>DIRECTIVE 2006/24</b>	265

8.1	APPROPRIATE LEGAL BASIS	265
8.2	SCOPE	266
8.3	LAWFULNESS	266
9	ARTICLES 7, 8 CFR	267
10	ARTICLE 8 ECHR	269
	<b>APPENDIX 1: RECITALS [1 to 173]</b>	271
	<b>APPENDIX 2: EU/EEA NATIONAL SUPERVISORY AUTHORITIES</b>	328
	<b>APPENDIX 3: LOOPHOLES IN GDPR</b>	330
	<b>APPENDIX 4: FLOW CHART – COMPOSITION OF EUROPEAN DATA PROTECTION BOARD</b>	342

## **PREFACE**

I was the early starter to get awakened towards GDPR due to my practice in cyber and privacy law. When I first started the firm EUGDPR Institute, I was sure about writing a book on GDPR but never knew the connotations it would have. I was involved in training participants from many large IT Companies like Tech Mahindra, TCS, Oracle, IBM, Cognizant etc. and obviously partners from large law firms then I decided to pen this book as the legal language and its interpretation was always a challenge to these technology or GRC migrants. Being author of published and famous books on cyber law made the structure of this book clear in my mind. Articles of GDPR do have a typical international law kinda language and often raises more than one questions or doubts in the avid reader of the topic.

This book is a series of articles and interpretations. It deals with questions of applicability of GDPR articles in various scenarios; at its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

Fundamentally, almost every aspect of our lives revolves around data. From social media companies, to banks, retailers, and governments -- almost every service we use involves the collection and analysis of our personal data. Your name, address, credit card number and more all collected, analysed and, perhaps most importantly, stored by organisations

In this busy age, when we are all bombarded with information, it is helpful, I think, to be offered a chance to take a breath and do things simply. There is something meditative about reading the GDPR articles one by one and again going through it next time. There is something therapeutic in watching people's faces light up when they find they are compliant to particular article of GDPR. There is something healing in the simple task of being aware about applicability of GDPR to the organisation. GDPR applies to any organisation operating within the EU, as well as any organisations outside of the EU, which offer goods or services to customers or businesses in the EU. That ultimately means that almost every major corporation and practitioner in the world will need this book to understand, implement, comply and re-comply with GDPR.



Whether you are a DPO, a auditor, a lawyer, a student, a GRC professional, a privacy devotee, a lonely heart nostalgic for GDPR trainings — I hope you find something of value in these pages. This book might inspire you to read your GDPR compliance report again, or it might just offer you an imaginative escape from the incessant hurry of modern day compliance requirements. Maybe it will prompt you to call your legal and compliance team. Regardless of how you use this book, I hope it helps you in some small way to build a data protection and privacy regime within your mind or in the organisation.

I Sincerely want to put on record my deep appreciation and salute to the team working on this book with special reference to Lawyer Tejal Patel, she has gone extra length to research and formalize the contents of this book.

Author

Prashant Mali [M.Sc. (Computer Science), LL.M]

Chevening Cyber Security Fellow (UK) & IVLP (USA)

Email: [cyberlawconsulting@gmail.com](mailto:cyberlawconsulting@gmail.com)

## **CHAPTER 1: GENERAL PROVISIONS**

### **Art. 1 GDPR Subject-matter and objectives**

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

### **Suitable Recitals**

(1) Data protection as a fundamental right; (2) Respect of the fundamental rights and freedoms; (3) Directive 95/46/EC harmonization; (4) Data protection in balance with other fundamental rights; (5) Cooperation between Member States to exchange personal data; (6) Ensuring a high level of data protection despite the increased exchange of data; (7) The framework is based on control and certainty; (8) Adoption into national law; (9) Different standards of protection by the Directive 95/46/EC; (10) Harmonised level of data protection despite national scope; (11) Harmonisation of the powers and sanctions; (12) Authorization of the European Parliament and the Council.

### **COMMENTARY:**

The European Union's (EU) view on data protection is closely linked to privacy issues, which does not appear to always be the right approach in dealing with data protection. The privacy concept as outlined in Art. 8 of the European Convention on Human Rights refers mainly to the right to private and family life, respect of private home and private correspondence. The data protection could include privacy issues but is not limited to them.

Data protection means the right of a person to know which data is gathered in regards to her person, how the data is used, aggregated, protected, and where the data is transmitted. Anyone has the right to have access to that data and to modify it. In all cases, the person has to give his/her consent for that data to be used by another person, government, or any other entity. Data protection values are not essentially privacy related ones. These values cannot be dealt with just through the privacy perspective. They are autonomous values, which grant fundamental rights: the right to data protection as recognised by Article 8 in the Charter of Fundamental Rights of the European Union: "Protection of personal data: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

The recognition of data protection by the EU legal framework constitutes an important step made towards the recognition of the Data Protection Directive, which for years has been perceived as having two main attributes: granting and protecting the free movement of personal information and the protection of fundamental rights and freedoms of an individual (from the privacy perspective). The recognition of the right to data protection given by the Charter, this could be considered as a way to give more weight to the fundamental rights dimension of the Directive. Some countries in the EU as such France and Germany, perceive privacy as not being related to data protection. Contrarily, other countries such as Belgium and The Netherlands, closely link together data protection to privacy. For this reason, recognising data protection as an individual freedom could help diminish the gaps in interpretation among EU Member States in this field.

Unfortunately, the EU legal framework regarding data protection is quite fragmented. The Directives regulating this area of data protection (Directive 95/46, Directive 2002/58, and Directive 2002/2) are overlapping, cover the same legal field and also have vague definitions (at least regarding the Location Based Services LBS). This comes against normal consumer-provider relations because the consumers will not be effectively and uniformly protected in their rights and the providers, by not knowing and understanding the regulations, will diminish or stop their service that goes against the consumer again because the choice of services in a field will be diminished.

The ruling of European Court of Justice (ECJ) in Case C-101/01, Bodil Lindqvist regarding data protection (the first of its kind), has important implications because it clarifies to individuals and companies that personal data is protected and no one can use it without prior authorization. This was a useful warning given by ECJ to those interested in using, manipulating, and accessing data, with no right or consent. It was a useful start, because since then more and more EU countries used this Directive in the right direction. Also, it was a clarification given to those countries, which did not know what the Directive 95/46/EC meant: data is protected not just through the privacy perspective but as a fundamental right as well.

Ruling on this case, ECJ tried to make a fair balance between fundamental rights and fundamental freedoms as well (the right to data protection and the freedom of expression). Dealing with these sensitive issues, it is always hard to make a decision regarding fundamental rights and harm fundamental freedoms and vice-versa. It is very hard to find the proper balance in ruling in these matters. One cannot acknowledge one fundamental right over another in a categorical manner. In this particular case the human right to data protection was definitely weighting more than the human right to freedom of expression in the ECJ's view, because someone's private information has the same value as someone's right to express his/her own beliefs, when that person uses a third party's private information with no consent. In this case, violating fundamental freedoms such data protection for the purpose of expressing personal beliefs was found to be wrong by the ECJ.

As a conclusion, data protection is a fundamental right and should be granted and protected as any other fundamental rights. Many people are not aware that the information concerning their person is protected which leads unfortunately to many abuses from authorities, internet providers, online businesses and many others. We all could hope that in time, following important ECJ rulings as the one described above, people will consider more and more seriously their fundamental right to data protection.

## **Art. 2 GDPR Material scope**

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

1. in the course of an activity which falls outside the scope of Union law;
2. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
3. by a natural person in the course of a purely personal or household activity;
4. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

## **Suitable Recitals**

(13) Taking account of micro, small and medium-sized enterprises; (14) Not applicable to legal persons; (15) Technology neutrality; (16) Not applicable to activities regarding national and common security; (17) Adaptation of Regulation (EC) No 45/2001; (18) Not applicable to personal or household activities; (19) Not applicable to criminal prosecution; (20) Respecting the independence of the judiciary; (21) Liability rules of intermediary service providers shall remain unaffected; (27) Not applicable to data of deceased persons.

## **COMMENTARY:**

The concept of 'personal data processing' is almost identical to that of the Directive, with two "operations" added ("structuring" and "restriction" that replaced

the “blocking”). The notion of “filing system” is strictly identical, namely “any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis” (Art. 4, 2).

This Directive was applied to the processing of personal data, wholly or partly automated, and to the non-automated processing of personal data contained or referred to in a file processed by either the public or the private sector.

The concept of automatic processing covered manual records, from the moment where the data are contained or are intended to be contained in a file. The definitions helping to understand the material scope were therefore logically focused on the concept of “personal data” (Art. 2a), “personal data processing” (Art. 2b) and “personal data filing system” (Art. 2 c).

Article 3, paragraph 2 of the Directive provided two exceptions to its scope: the first exception applied to processing in the course of an activity which falls outside the scope of Community law, such as those related to public security, defence, state security and the activities of the state in areas of criminal law. The second exception provided for in Article 3, paragraph 2, also deals with the processing by a natural person for the exercise of purely personal or household activities, such as correspondence and maintaining of directories of addresses.

### **Art. 3 GDPR Territorial scope**

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

1. The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
2. the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

### **Suitable Recitals**

(22) Processing by an establishment; (23) Applicable to processors not established in the Union if data subjects within the Union are targeted; (24) Applicable to processors not established in the Union if data subjects within the Union are profiled; (25) Applicable to processors due to international law.

## COMMENTARY

The GDPR will apply to organizations which have EU “establishments”, where personal data are processed “in the context of the activities” of such an establishment. If this test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not. “Establishment” was considered by the Court of Justice of the European Union (“CJEU”) in the 2015 case of *Weltimmo v/s NAIH* (C-230/14). This confirmed that establishment is a “broad” and “flexible” phrase that should not hinge on legal form. An organisation may be “established” where it exercises “any real and effective activity – even a minimal one” – through “stable arrangements” in the EU. The presence of a single representative may be sufficient. In that case, *Weltimmo* was considered to be established in Hungary as a result of the use of a website in Hungarian which advertised Hungarian properties (which meant that, as a consequence, it was considered “mainly or entirely directed at that Member State”), use of a local agent (who was responsible for local debt collection and acted as a representative in administrative and judicial proceedings), and use of a Hungarian postal address and bank account for business purposes – notwithstanding that *Weltimmo* was incorporated in Slovakia.

Organisations which have EU sales offices, which promote or sell advertising or marketing targeting EU residents will likely be subject to the GDPR – since the associated processing of personal data is considered to be “inextricably linked” to and thus carried out “in the context of the activities of” those EU establishments (*Google Spain SL, Google Inc. v AEPD, Mario Costeja Gonzalez* (C-131/12)).

### **Non-EU “established” organisations who target or monitor EU data subjects**

Non-EU established organisations will be subject to the GDPR where they process personal data about EU data subjects in connection with:

- the “offering of goods or services” (payment is not required); or
- “monitoring” their behaviour within the EU.

For offering of goods and services (but not monitoring), mere accessibility of a site from within the EU is not sufficient. It must be apparent that the organisation “envisages” that activities will be directed to EU data subjects. Contact addresses accessible from the EU and the use of a language used in the controller’s own country are also not sufficient. However, the use of an EU language/currency, the ability to place orders in that other language and references to EU users or customers will be relevant.

The CJEU has examined when an activity (such as offering goods and services) will be considered “directed to” EU Member States in a separate context (i.e. under the “Brussels 1” Regulation (44/2001/EC) governing “jurisdiction...in civil and commercial matters”). Its comments are likely to aid interpretation under this similar aspect of the GDPR. In addition to the considerations mentioned above, the CJEU notes that an intention to target EU customers may be illustrated by: (1)

“patent” evidence, such as the payment of money to a search engine to facilitate access by those within a Member State or where targeted Member States are designated by name; and (2) other factors – possibly in combination with each other – including the “international nature” of the relevant activity (e.g. certain tourist activities), mentions of telephone numbers with an international code, use of a top-level domain name other than that of the state in which the trader is established (such as .de or .eu), the description of “itineraries...from Member States to the place where the service is provided” and mentions of an “international clientele composed of customers domiciled in various Member States”. This list is not exhaustive and the question should be determined on a case-by-case basis (*Pammer v/s Reederei Karl Schluter GmbH & Co* and *Hotel Alpenhof v/s Heller* (Joined cases (C-585/08) and (C-144/09))).

It is not clear whether non-EU organisations offering goods and services to EU businesses (as opposed to individuals) will fall within the scope of the “offering goods and services” test in Article 3(2)(a). Monitoring” specifically includes the tracking of individuals online to create profiles, including where this is used to take decisions to analyse/predict personal preferences, behaviours and attitudes. Organisations subject to the GDPR’s long-arm jurisdictional reach must appoint an EU-based representative.

Under the Data Protection Directive, organisations targeting EU data subjects only had to comply with EU rules if they also made use of “equipment” in the EU to process personal data. This led national supervisory authorities, who were seeking to assert jurisdiction, to develop arguments that the placing of cookies, or requesting users to fill in forms, would amount to the use of “equipment” in the EU. It will now be easier to demonstrate that EU law applies. (Although, where organisations have no EU presence, enforcement may be just as difficult as before).

## **Exclusions**

Certain activities fall entirely outside the GDPR’s scope (listed below):

In addition, the GDPR acknowledges that data protection rights are not absolute and must be balanced (proportionately) with other rights – including the “freedom to conduct a business”. (For the ability of Member States to introduce exemptions, see section on derogations and special conditions). As the GDPR toughens up many areas of data protection, introducing more new sticks than regulatory carrots, businesses may find it helpful to bookmark this statement in Recital 4 in case of future need.

The GDPR does not apply to the processing of personal data (these general exemptions are very similar to the equivalent provisions included in the Data Protection Directive):

- in respect of activities which fall outside the scope of EU law (e.g. activities concerning national security);
- in relation to the EU’s common foreign and security policy;

- by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences and associated matters (i.e. where the Law Enforcement Agencies (“LEA”) Directive, which was adopted as EU 2016/618 on 26 April 2016 now applies);
- by EU institutions, where Regulation 45/2001/EC will continue to apply instead of the GDPR. This Regulation is to be updated to ensure consistency with the GDPR; and
- by a natural person as part of a “purely personal or household activity”. This covers correspondence and the holding of address books – but it also now covers social networking and online activities undertaken for social and domestic purposes. It represents a possible widening of the exemption from the principles set out in *Bodil Lindqvist* (C-101/01), before the advent of social media. In this case, the CJEU noted that sharing data with the Internet at large “so that those data are made accessible to an indefinite number of people” could not fall within this exemption, which it stated should be limited to activities “carried out in the course of the private or family life of individuals”. Note also that the GDPR will remain applicable to controllers and processors who “provide the means for processing” which falls within this exemption.

The GDPR is stated to be “without prejudice” to the rules in the E-commerce Directive (2000/31/EC), in particular to those concerning the liability of “intermediary service providers” (and which purport to limit their exposure to pecuniary and criminal liability where they merely host, cache or act as a “mere conduit”). The relationship with the E-commerce Directive is not straightforward – as that Directive states that issues relating to the processing of personal data are excluded from its scope and “solely governed” by relevant data protection legislation. The two can be read consistently if one assumes that the liability of ISPs for the actions of users will be determined by the E-commerce Directive, but that other matters (such as obligations to erase or rectify data, or obligations on an ISP concerning its own uses of personal data) will be governed by the GDPR. However, the point is not clear.

Determining an organization’s applicability under the General Data Protection Regulation is a complex topic, and many are left a bit confused while researching applicability under the monumental regulation. Oftentimes, there’s conflicting information as to whether it applies to a specific organization. The expansive coverage of the GDPR by itself can be intimidating, but, by breaking down the fundamentals into smaller, more manageable sections, we can start making better decisions on its applicability and craft a compliance framework based on a solid foundation. Before we jump into the requirements, it’s important to note that this criteria below is applicable to organizations even where the processing of personal data takes place outside of the EU. Due to that international reach, one cannot simply avoid GDPR obligations because they are outside the jurisdiction of the EU. So, let’s begin to dissect the parts of Article 3 and its provisions under “territorial scope” to get a better understanding of how GDPR classifies an “in-scope”



organization, along with the two conditions that decide the applicability of an organization in the eyes of the regulation.

**Criterion 1: If your business is offering goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU**

The definition of "offering of goods and services" isn't extraordinarily specific when referring to Article 3. In general, websites are globally accessible. So, would that mean your business is, by default, offering goods and services to EU citizens? Looking further into the GDPR's clarification under Recital 23 provides a better perception of how it's interpreted according to the regulation.

According to the above text from the GDPR, organizations may demonstrate "intention of offering goods and services" to EU citizens under the following circumstances:

- The organization provides the option to interact with the website in the native language and currency of an EU Member State; and/or
- The organization advertises its customers or users (i.e. testimonials) that are in based in the union with the goal of appealing to other users in the same locality.

The Court Justice of the European Union offers good clarification on the topic of "intention" in relation to offering your product to EU citizens, and how it can be demonstrated under the following conditions:

- "Patent" evidence, such as the payment of money to a search engine to facilitate access by those within a member state or where targeted member states are designated by name;
- Other factors — possibly in combination with each other — including the "international nature" of the relevant activity (e.g. certain tourist activities), mentions of telephone numbers with an international code, use of a top-level domain name other than that of the state in which the trader is established (such as .de or .eu), the description of "itineraries ... from member states to the place where the service is provided," and mentions of an "international clientele composed of customers domiciled in various member states."

Drawing from the main points in the above statements, it should be noted that organizations should further examine their obligations under the regulation where they:

- Include international telephone numbers on their website for contact purposes;
- Use top level domains of an EU Member State (i.e. .eu, .ie, .de);
- Provide options for EU language translation;
- Provide options for EU currency conversion; and,
- Advertising to attract EU users (leveraging existing EU clients or users as advertising material).

If your organization meets at least one of the above criterion, it may be a good time to prompt a review and determine if you're required to comply with GDPR's requirements. Where in doubt, always seek legal advice.

**Criterion 2: If your business monitors the behavior of EU citizens and their behavior takes place within the union.**

The regulation also uses the word “monitoring” in relation to organizations’ processing activities and may be unclear as to its true meaning and how it applies. To gain better understanding, we can use guidance provided by Recital 24 of the regulation; specifically, “natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.”

The above excerpt appears to refer to online monitoring and could be associated with behavioral-based advertising that creates profiles based on the data subject’s actions. Monitoring in the GDPR framework is also referred to as “profiling,” and is defined as the automated analysis or predicting of behavior, location, movements, reliability, interests, personal preferences, health, economic situation, performance, etc. It’s also important to note that Article 29 Working Party does provide other examples of monitoring including, but not limited to:

- Online behavioral based advertising;
- Travel data of individuals using a city’s public transport system (e.g. tracking via travel cards);
- Profiling and scoring for purposes of risk assessment (e.g. for purposes of credit scoring, establishment of insurance premiums, fraud prevention, detection of money-laundering);
- Location tracking, for example, by mobile apps; and
- Monitoring of wellness, fitness and health data via wearable devices.

Article Working Party 29 suggests that organizations should consider all forms of behavior monitoring, including CCTV, smart cars, home automation, etc. With the wide scope of profiling behavior, organizations should evaluate their current online and offline operations to determine if they will be classified under the monitoring requirement. Organization should also consider “monitoring” in circumstances where they collect data on their employees inside and outside of the workplace, including BYODs, MDM solutions that track location and company owned vehicles with tracking devices. Clearly, given the wide net this regulation captures, information technology leaders and process owners of all organizations should prioritize assessing a formal conclusion on GDPR’s applicability, as the deadline is almost upon us. If you are unsure if your organization falls into scope of Article 3’s criteria, you should seek the advice from a privacy expert and your legal advisors.

## **Art. 4 GDPR Definitions**

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
4. 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6. 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall

be in compliance with the applicable data protection rules according to the purposes of the processing;

10. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. ‘main establishment’ means:

- a. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
- b. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

- a. the controller or processor is established on the territory of the Member State of that supervisory authority;
- b. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
- c. a complaint has been lodged with that supervisory authority;

23. ‘cross-border processing’ means either:

- a. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- b. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council;

26. ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

**Suitable Recitals**

(15) Technology neutrality; (24) Applicable to processors not established in the Union if data subjects within the Union are profiled; (26) Not applicable to anonymous data ;(28) Introduction of Pseudonymisation; (29) Pseudonymisation at the same controller; (30) Online identifiers for profiling and identification; (31) Not applicable to public authorities in connection with their official tasks; (34) Genetic data; (35) Health data; (36) Determination of the main establishment; (37) Enterprise group.

\* \* \*

## **CHAPTER 2: PRINCIPLES**

### **Art. 5 GDPR Principles relating to processing of personal data**

1. Personal data shall be:
  - a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
  - b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
  - c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  - d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
  - e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
  - f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

#### **Suitable Recitals**

(39) Principles of data processing.

#### **COMMENTARY:**

The principles are set in article 5 of the GDPR and enshrined thorough all the Regulation, and they apply to every personal data processing activity. As the cornerstone of the Regulation, they should be kept in mind when interpreting the rights and duties established in the GDPR.

## 1. Lawfully, Fairly and Transparent

**Lawfully** refers to the duty to process personal data only when there is an appropriate legal basis or legislative measure under the GDPR, EU, or Member State Law. Strictly speaking only when you count with legitimate grounds to process personal data, e.g., explicit consent, you can collect and carry out the processing activities. In that sense, situations, where the collection of personal data has been done by a non-authorised access, would be unlawful and therefore contrary to this principle. Relevant references: Articles 5, 6, 9 and 10 / Recitals: 39, 45 and 63.

**Fairly**, requires providing sufficient information to the data subject to make the processing fair and transparent. In particular, the data subject needs to be informed of the existence of the processing activities and its purposes at the moment of collection. The information shall include all necessary details to ensure fairness and transparent processing, taking into account the specific circumstances and context in which the personal data is processed. If it is the case, the data subject should be informed of the existence of profiling and consequences and any legal obligation on the data subject to provide with him/her personal data and its consequences if he or she does not do so. Relevant references: Article 5 and 6 / Recitals: 39, 45, 60 and 71.

**Transparent**, refer to the responsibility to ensure that any information or communication to the data subject shall be concise, easily accessible and easy to understand – clear and plain language; especially when is addressed to a child. Furthermore, to ensure a fair and transparent processing, this duty concerns the information that should be accessible to the data subject. By rule, all natural persons should be made aware of risk, rules, safeguards, and rights concerning the processing of him/her personal data and how to exercise their rights to such activities. Relevant references: Articles: 5, 12 to 22 and 34 / Recitals: 39, 58 to 63 and 71.

## 2. Purpose Limitation

This principle can be divided in two:

- personal data may only be collected for specified (defined), explicit (clear) and legitimate purposes (legal basis) determined at the moment of collection. Undefined and/or unlimited purposes is unlawful;
- personal data must only be processed in a manner compatible with those purposes. Otherwise, it is required a new and separate legal basis.

Now, there are two specific exemptions to this principle:

- 89(1) processing for archiving, scientific, historical or statistical purposes as far as appropriate technological and organizational measures are in place to protect the rights and freedoms of the data subjects, in particular, the principle of data minimisation.
- 6(4) processing for another purpose compatible with the purpose for which the personal data are initially collected. To assess the compatibility the following



points should be considered: (i) the fair processing information the controller initially provided to the data subject; (ii) the relationship between the purposes for which the data have been collected and the purposes of further processing; (iii) the context in which the data were collected and the reasonable expectations of the data subjects as to their further use; (iv) the nature of the data and the impact of the further processing on the data subjects; and (v) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Relevant references: Article 5 and 6 / Recitals 39, 45 and 50.

### **3. Data Minimization**

This principle refers to the duty to process personal data only when it is adequate (appropriate), relevant (pertinent) and limited to what is necessary for the purposes for which they are processed (not excessive). To limit the storage of the personal data to a strict minimum, there is a need to establish time limits to delete data or to have periodic reviews to assess what should be erased. Also, to respect data minimisation an assessment should be made regarding the need to process personal data since if there is another reasonable privacy-friendly solution that can fulfill the purposes, the personal data shouldn't be handled. Relevant references: Article 5 and 25 / Recitals 39 and 156.

### **4. Accuracy**

This principle imposes the responsibility to take every reasonable step to ensure that personal data are accurate and up to date concerning the specific purposes for which they are processed. Inaccurate data shall be erased or rectified without delay. Attention should be given to the word "reasonable", the steps required shouldn't be something that would involve a disproportionate effort. Relevant references: Articles 5 and 18 / Recital 39.

### **5. Storage Limitation**

This principle refers to the obligation to keep the personal data as far as necessary to identify the data subjects for the purposes established. In that sense, the data retention has to be set in a way that personal data is erased when the purposes have been served. Now, there is one specific exemption to this principle:

- 89(1) processing for archiving, scientific, historical or statistical purposes as far as appropriate technological and organizational measures is in place to protect the rights and freedoms of the data subjects, in particular, the principle of data minimisation.

Relevant references: Articles 5, 6, 23 and 25 / Recital 39 and 45.

### **6. Integrity and Confidentiality**

This principle establishes the duty to process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical

or organisational measures. Relevant references: Articles 5 and 32 / Recital 74 to 84, 94 and 95.

## **7. Accountability**

This principle states the obligation to comply with the principles and to be able to demonstrate that processing is performed in accordance with them. Relevant references: Articles 5 and 24.

### **Final Notes:**

- The obligations to comply with the principles rely on the Data Controller(s). However, the Data Processor(s) shall observe them and act accordingly – keep in mind the Data Processor's obligation under article 28 (3)(h) GDPR.
- Union or Member State Law may restrict by way of legislative measure the scope of article 5 as long as its provisions correspond to the rights and obligations provided in articles 12 to 22, and such restrictions respect the essence of the fundamental rights and freedoms and is necessary and proportionate measure in a democratic society to safeguard: national security, defence, public security, etc.
- It's no secret that we might find regulatory gaps because of the technological developments. Keep pace with the times is not an easy task, but I trust our authorities would provide with more light regarding the many interfaces that are between law, regulation, and technology.

## **Art. 6 GDPR Lawfulness of processing**

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c. processing is necessary for compliance with a legal obligation to which the controller is subject;
- d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

- a. Union law; or
- b. Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

- a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
- d. the possible consequences of the intended further processing for data subjects;

e. the existence of appropriate safeguards, which may include encryption or Pseudonymisation.

### **Suitable Recitals**

(39) Principles of data processing; (40) Lawfulness of data processing; (41) Legal basis or legislative measures; (42) Burden of proof and requirements for consent; (43) Freely given consent; (44) Performance of a contract; (45) Fulfillment of legal obligations; (46) Vital interests of the data subject; (47) Overriding legitimate interest; (48) Overriding legitimate interest within group of undertakings; (49) Network and information security as overriding legitimate interest; (50) Further processing of personal data; (171) Repeal of Directive 95/46/EC and transitional provisions.

### **COMMENTARY:**

Article 6(1) GDPR sets out the conditions that must be satisfied for the processing of personal data to be lawful (For provisions relating to sensitive data see section on sensitive data and lawful processing). These grounds broadly replicate those in the Data Protection Directive. These are:

#### **6(1)(a) – Consent of the data subject**

The GDPR approaches consent more restrictively; in particular it seeks to ensure that consent is specific to distinct purposes of processing (see section on consent). Particular conditions are imposed in the case of children online (See section on children).

#### **6(1)(b) – Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract**

No change to the position under the Data Protection Directive.

#### **6(1)(c) – Necessary for compliance with a legal obligation**

This replicates an equivalent ground under the Data Protection Directive. However, Article 6(3) and Recitals 41 and 45 make it clear that the legal obligation in question must be:

- an obligation of Member State or EU law to which the controller is subject; and
- “clear and precise” and its application foreseeable for those subject to it.

The recitals make it clear that the relevant “legal obligation” need not be statutory (i.e. common law would be sufficient, if this meets the “clear and precise” test). A legal obligation could cover several processing operations carried out by the controller so that it may not be necessary to identify a specific legal obligation for each individual processing activity.

#### **6(1)(d) – Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent**

Recital 46 suggests that this ground may apply to processing that is necessary for humanitarian purposes (e.g. monitoring epidemics) or in connection with

humanitarian emergencies (e.g. disaster response). The recital indicates that in cases where personal data are processed in the vital interests of a person other than the data subject, this ground for processing should be relied on only where no other legal basis is available.

### **6(1)(e) – Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller**

Article 6(3) and Recital 45 make clear this ground will apply only where the task carried out, or the authority of the controller, is laid down in Union law or Member State law to which the controller is subject.

### **6(1)(f) – Necessary for the purposes of legitimate interests**

This ground can no longer be relied on by public authorities processing personal data in the exercise of their functions; Recitals 47-50 add more detail on what may be considered a “legitimate interest”. Member States are permitted to introduce specific provisions to provide a basis under Articles 6(1)(c) and 6(1)(e) (processing due to a legal obligation or performance of a task in the public interest or in the exercise of official authority) and for other specific processing situations (e.g. journalism and research). This is likely to result in a degree of variation across the EU.

### **Further processing**

The GDPR also sets out the rules (at Article 6(4)) on factors a controller must take into account to assess whether a new processing purpose is compatible with the purpose for which the data were initially collected. Where such processing is not based on consent, or on Union or Member State law relating to matters specified in Article 23 (general article on restrictions relating to the protection of national security, criminal investigations etc.), the following factors should be taken into account in order to determine compatibility:

- any link between the original and proposed new purposes;
- the context in which data have been collected (in particular the relationship between subjects and the controller);
- the nature of the data (particularly whether they are sensitive data or criminal offence data);
- the possible consequences of the proposed processing; and
- the existence of safeguards (including encryption or Pseudonymisation).

## **Art. 7 GDPR Conditions for consent**

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration, which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

### **Suitable Recitals**

(32) Conditions for consent; (33) Consent to certain areas of scientific research; (42) Burden of proof and requirements for consent; (43) Freely given consent.

### **COMMENTARY:**

One of the major areas of change—and the one that's been causing email marketers the biggest headache—is the question of how to collect and store consent. GDPR raises the bar to a higher standard of consent for subscribers based in the EU, meaning that the way your brand has collected consent from EU subscribers in the past might not be compliant anymore. GDPR goes beyond the consent required under the EU Privacy Directive, which is currently in effect across the EU. The new regulation requires that brands collect affirmative consent that is “freely given, specific, informed and unambiguous” to be compliant.

### **Few things you must know about e-mail consent under GDPR**

#### **1. KEEP EVIDENCE OF CONSENT—WHO, WHEN, HOW.**

GDPR not only sets the rules for how to collect consent, but also requires companies to keep a record of these consents.

**Article 7 (1):** “Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.”

In some countries, the burden of proving consent has always been the responsibility of the company that collected the opt-in. For many other marketers, however, this requirement is a new challenge to tackle.

Keeping evidence of consent means that you must be able to provide proof of:

- Who consented
- When they consented
- What they were told at the time of consent

- How they consented (e.g., during checkout, via Facebook form, etc.)
- Whether they have withdrawn consent

## **2. MAKE IT EASY FOR PEOPLE TO WITHDRAW CONSENT—AND TELL THEM HOW TO DO IT.**

**Article 7(3):** “The data subject shall have the right to withdraw his or her consent at any time. It shall be as easy to withdraw as to give consent.”

All major email laws, including CASL in Canada and CAN-SPAM in the U.S., require brands to give their subscribers the opportunity to opt out from receiving emails. Each promotional email you send must include an option to unsubscribe. If you are already compliant with current Canadian, American, or European email laws, you may not have to change much when it comes to this requirement for GDPR compliance. Still, this is a perfect time to revisit your current opt-out process to ensure you’re following best practices:

- Don’t charge a fee
- Don’t require any other information beyond an email address
- Don’t require subscribers to log in
- Don’t ask subscribers to visit more than one page to submit their request

## **3. KEEP CONSENT REQUESTS SEPARATE FROM OTHER TERMS & CONDITIONS.**

Email consent must be freely given—and that’s only the case if a person truly has a choice of whether or not they’d like to subscribe to marketing messages. If subscribing to a newsletter is required in order to download a whitepaper, for example, then that consent is not freely given. Under GDPR, email consent needs to be *separate*. Never bundle consent with your terms and conditions, privacy notices, or any of your services, unless email consent is necessary to complete that service.

**Article 7(4):** “When assessing whether consent is freely given, utmost account shall be taken of whether... the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”

## **4. CONSENT REQUIRES A POSITIVE OPT-IN. DON’T USE PRE-TICKED BOXES.**

For consent to be valid under GDPR, a customer must actively confirm their consent, such as ticking an unchecked opt-in box. Pre-checked boxes that use customer inaction to assume consent aren’t valid under GDPR.

## **5. CHECK YOUR CONSENT PRACTICES AND YOUR EXISTING CONSENTS.**

**Recital 171:** “Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation.”

GDPR does not only apply to signups that happen after May 25<sup>th</sup>, it applies to *all existing EU subscribers* on your email list. If your existing subscribers have given you consent in a way that's already compliant with GDPR—and if you kept record of those consents—there's no need for you to re-collect consent from those subscribers. If your existing records don't meet GDPR requirements, however, you have to take action.

### **1. Audit your existing email list.**

Figure out who on your email list already provided GDPR-compliant consent, and ensure that you have a clear record of those consents.

### **2. Implement a re-permission program**

If for any of your contacts you don't have GDPR-proof consent—or if you are unsure about whether or not their consent is compliant—you'll have to run a re-permission campaign to refresh that consent, or remove the subscriber from your mailing list.

## **Art. 8 GDPR Conditions applicable to child's consent in relation to information society services**

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

### **Suitable Recitals**

(38) Special protection of children's personal data.

### **COMMENTARY:**

## **GDPR IMPLEMENTATION IN RESPECT OF CHILDREN'S DATA**

1. While Article 8 of the GDPR imposes specific conditions to a child's consent in relation to the offer of information society services directly to a child, other legal processing bases are still applicable and sometimes more appropriate to the processing of children's data.

2. The offer of an information society service directly to a child neither means "offered exclusively" to a child nor does it mean "made available" to a child. Rather,



it is a contextual determination that must be made through an appropriate risk-based test.

3. A risk-based test to determine whether an information society service is offered directly to a child should be developed within the framework of the GDPR, taking into account whether the offering is made intentionally attractive to children.

4. A widely recognised, effective and reliable method of parental verification, which can be applied globally should be supported by regulators and developed together with industry.

5. Where the holder of parental responsibility gives or authorises consent for processing a child's personal data under Article 8, such consent should remain valid when the child attains the age of digital consent.

6. Organisations should have the flexibility to provide transparency and notices in the way they think is most appropriate to cater to their specific audience, taking into account that the audience may include young children.

7. In general, the processing of personal data of children for advertising to them is not sufficient to rate the processing as high risk and there should be no preconceived notion to the contrary.

8. The importance of a consistent approach to implementing national age thresholds should be emphasised by data protection authorities in line with the GDPR's goal of harmonisation. This is particularly relevant as Member States finalise their national data protection laws implementing the GDPR.

9. The age at which children can exercise their rights under the GDPR (apart from consent under Article 8) turns on questions of competence, which are issues of Member State law.

Providers of information society services, which fall within the scope of Article 8, should be permitted to rely on legitimate interest for the continuation of services to children, who previously consented to processing by the service, after 25<sup>th</sup> May 2018, provided the requirements surrounding the use of the alternative legal basis are met.

## **Art. 9 GDPR Processing of special categories of personal data**

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

a. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law

provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. Processing relates to personal data which are manifestly made public by the data subject;

f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim

pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

### **Suitable Recitals**

(46) Vital interests of the data subject; (51) Protecting sensitive personal data; (52) Exceptions to the prohibition on processing special categories of personal data; (53) Processing of sensitive data in health and social sector; (54) Processing of sensitive data in public health sector; (55) Public interest in processing by official authorities for objectives of recognized religious communities; (56) Processing personal data on people's political opinions by parties.

### **COMMENTARY:**

#### **Special data under the GDPR vs. Sensitive data under the DPD**

With regard to special data, the changes appear, at first glance, to be minor. The GDPR refers to sensitive personal data as “special categories of personal data” (Article 9 of the GDPR). These categories are broadly the same as those in the DPD, except that sensitive data now specifically includes; “genetic data” and “biometric data”, where processed “to uniquely identify a person”. Personal data relating to criminal convictions and offences are not included in those categories, but similar extra safeguards apply to their processing under the GDPR as are currently in effect under the DPD (Article 10 of the GDPR).

Article 9.2 sets out the circumstances in which the processing of “special categories of personal data”, otherwise prohibited, may occur. These grounds largely replicate those under the DPD, which are principally: the explicit consent of the data subject, the performance of specific contracts or processing for specific purposes (e.g. vital interest of an individual or public interest in the area of health, employment, social security, etc.).

Pursuant to these provisions, data controllers must be able to demonstrate that they have a legal basis for the processing of special data. However, the GDPR introduces a new requirement in its Article 35 to perform a Privacy Impact Assessment (PIA) when a type of processing is likely to result in a high risk to the rights and freedoms of data subjects. PIAs are mandatory in the case of large-scale processing of special categories of data (Article 35.3 (b) of the GDPR). Furthermore,

Article 36.1 specifies that the data controller must consult the competent Data Protection Authority prior to starting the processing when the PIA indicates that such processing is likely to result in a high risk to individuals in the absence of measures taken by the data controller to mitigate such risk.

This means that under the GDPR, having a legal basis, such as the consent of the data subject, will no longer be sufficient to process special personal data in cases where the risk to individuals is high, unless the relevant Data Protection Authority sanctions the processing.

## **Health data**

Of all the categories of special data, health-related information - very sensitive in nature - is of particular interest with the increasing use of big data analytics and new technologies in the health and 'wellness' sectors. Here, the changes are more significant. It is to be noted that there are a number of exceptions to the restrictions on processing health data under Article 9.2, including where the processing is necessary for various medical assessments and where the processing is necessary for reasons of public interest in public health.

Also, Member States are entitled, under Article 9(4) GDPR, to maintain or impose further conditions (including limitations) in respect of genetic, biometric or health data. As such, existing differences in approach on these topics will likely be maintained, and further divergence across Member States will be permitted. France already has its own regime under which (i) the processing of health data requires a preliminary declaration or authorisation regime, and (ii) a very specific set of policies and regulation for organisations which host such data has been created.

The GDPR introduces a wide definition of health data: “Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test” (Recital 35). This new definition will help processors and controllers to identify whether the data they collect constitutes health data in order to implement adequate safeguards and document their records adequately. All organisations processing special data will need to become well acquainted with the new EU data protection rules as well as relevant national law and review their existing policies, procedures, and practices to ensure compliance.

## **Art. 10 GDPR Processing of personal data relating to criminal convictions and offences**

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

### **Suitable Recitals**

(50) Further processing of personal data.

### **COMMENTARY:**

Article 10 means you must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill. We will publish more detailed guidance on the conditions in the Bill once these provisions are finalised. Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

### **At a glance**

- To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.
- The Data Protection Bill deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.
- You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.
- You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.
- You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

### **What's new?**

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10. Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

## **What is criminal offence data?**

Article 10 applies to personal data relating to criminal convictions and offences, or related security measures. In this guidance, we refer to this as criminal offence data. This concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act. However, it is potentially broader than this. In particular, Article 10 specifically extends to personal data linked to related security measures.

## **What's different about criminal offence data?**

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that if you are processing personal criminal offence data, you will also need to comply with Article 10.

## **Art. 11 GDPR Processing which does not require identification**

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

## **Suitable Recitals**

(57) Additional data for identification purposes.

## **COMMENTARY:**

If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

\* \* \*

## CHAPTER 3: RIGHTS OF THE DATA SUBJECT

### Section 1: Transparency and modalities

#### **Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject**

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- a. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- b. refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

### **Suitable Recitals**

(58) The principle of transparency; (59) Procedures for the exercise of the rights of the data subjects; (60) Information obligation; (73) Restrictions of rights and principles.

### **COMMENTARY:**

#### **Rights of Data Subjects under the GDPR**

All natural persons whose personal data is processed by a Data Controller (DC) or Data Processor (DP) within the territorial scope of the GDPR, are Data Subjects and hence entitled to these rights. The DC is the responsible for allowing data subjects to exercise their rights and to ensure that they can make effective use of them. In that sense, it's not only allowing the data subjects to exercise their rights but also to ensure the effectiveness. For instance, to allow a Data Subject to object the processing without providing all the information about the processing, wouldn't ensure the effective use of his/her right. Also, the DP shall observe and commit with the protection of the data subjects' rights in line with article 28 (3)(h) GDPR.

#### **The modalities applicable for the exercise of the rights**

Provide all the information relating to the processing of their personal data in a clear and understandable language, free of charge and without undue delay and in any event within 1 month of receipt of the request. Main Recital: 58 and 59 / Restrictions: Art.12 (2) and (5) (b)

#### **Recital 58 The principle of transparency**

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in



situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

### **Recital 59 Procedures for the exercise of the rights of the data subjects**

Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

## **Section 2: Information and access to personal data**

### **Art. 13 GDPR Information to be provided where personal data are collected from the data subject**

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

1. The identity and the contact details of the controller and, where applicable, of the controller's representative;
2. The contact details of the data protection officer, where applicable;
3. The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
5. The recipients or categories of recipients of the personal data, if any;
6. Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

1. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  2. The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
  3. Where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  4. The right to lodge a complaint with a supervisory authority;
  5. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
  6. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

### **Suitable Recitals**

(60) Information obligation; (61) Time of information; (62) Exceptions to the obligation to provide information.

### **COMMENTARY:**

Article 13 of the Regulation increases the obligation of notification when the data is collected from the data subject unless he/she already has the relevant information. The obligatory elements of information already presented in the Directive are diversified: the information given should serve to identify the possible delegate to the data protection, any representative of the controller, the legal basis and the purpose of processing or the legitimate interests on which the controller is based. Other mandatory information includes the will to make a transfer of data to a recipient in a third country or an international organization, the lack of decision on adequacy of the level of protection or, if appropriate, the reference to the appropriate

or adequate safeguards and the ways to obtain a copy or where they were made available.

The concept of recipient must be understood as a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not; public authorities which may receive personal data in the framework of a particular inquiry in accordance shall not be regarded as recipients (Art. 4 (9)). The obligation to notify the other elements of information is required to ensure "fair and transparent processing" which should change nothing in substance.

On the contrary, the elements of information are more numerous. Now it also includes in particular the period of data storage, or at least the criteria for determining the existence of all the rights of a person (including for example the right to data portability or withdrawal of consent), and the right to lodge a complaint with a supervisory authority.

The possible compulsory nature of the collection results in the highest precision (regulatory or contractual nature of the requirement of providing the data, including consequences on the conclusion of a contract for the provision of data, etc.). The controller should also, where appropriate, notify about the existence of any automated decision-making, including profiling under Articles 22 (1) and (4) as well as significant information of the underlying logic and consequences of the processing for the data subject.

Where appropriate, the changes of the purposes of processing data against the initial purpose must also be notified which means, if appropriate, new preliminary information on all of the above elements. Article 10 of the Directive provided for an obligation to notify the data subject that is differently implemented depending on whether the data are collected directly from the data subject or from a third party.

#### **Art. 14 GDPR Information to be provided where personal data have not been obtained from the data subject**

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- a. The identity and the contact details of the controller and, where applicable, of the controller's representative;
- b. The contact details of the data protection officer, where applicable;
- c. The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- d. The categories of personal data concerned;
- e. The recipients or categories of recipients of the personal data, if any;
- f. Where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or

absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- a. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- b. Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- c. The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- d. Where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- e. The right to lodge a complaint with a supervisory authority;
- f. From which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- g. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

- a. Within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- b. If the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- c. If a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

- a. The data subject already has the information;

- b. The provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- c. Obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- d. Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

### **Suitable Recitals**

(60) Information obligation; (61) Time of information; (62) Exceptions to the obligation to provide information.

### **COMMENTARY:**

In its Article 14, the Regulation reinforces the obligations to provide information when the data were not collected from the data subject, while extending the general exceptions. The obligatory elements of information already presented in the Directive are diversified: the information given should serve to identify the possible delegate to the data protection and the legal basis and indicate the purpose of processing or the legitimate interests on which the controller is processing data. Other mandatory information includes the will to make a transfer of data to a recipient in a third country or an international organization, the lack of decision on adequacy of the level of protection or, if appropriate, the appropriate or adequate safeguards provided and the ways to obtain a copy. The obligation to notify the other elements of information is necessary to ensure "fair and transparent processing" which should change nothing in substance.

On the other hand, the elements of information are more numerous.

Now it also includes in particular the period of data storage, or at least the elements allowing for determining it, the identification of the legitimate interests in case of lawfulness based on a balance of interests, rights and freedoms (Art. 6 (1), (f) of the Regulation), the existence of all the rights recognized to a person (including for example the right to data portability or withdrawal of consent), and the right to lodge a complaint with a supervisory authority. And finally, the sources that the data come from, including the sources that are publicly available are covered.

Where appropriate, the existence of any automated decision-making including profiling under Articles 22 (1) and (4) as well as significant information of the

underlying logic and consequences of the processing for the data subject shall also be notified. The Regulation also specifies that the controller must provide this information to the data subject either within a reasonable time not exceeding one month after the collection or, if it is envisaged to provide the information to another person or to use the data for communication to the data subject, when the information is communicated for the first time at the latest.

Where appropriate, the changes of the purposes for processing data against the initial purpose must also be notified which means, if appropriate, new information on all of the above elements. Exceptions are provided for. The information must not be provided if the data subject already has the information, if proven to be impossible or would require disproportionate efforts. There are clarifications concerning processing for archiving purposes in the public interest as well as for scientific purposes, historical or statistical research. Another exception is provided in the case of obtaining or communicating the information if subject to specific provisions in EU law or national law or if the data must remain confidential, subject to an obligation of professional secrecy in accordance with the EU law or the law of a Member State.

Articles 10 and 11 of the Directive provided for an obligation to notify the data subject that was differently implemented depending on whether the data were collected directly from the data subject or from a third party.

### **Art. 15 GDPR Right of access by the data subject**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- a. The purposes of the processing;
- b. The categories of personal data concerned;
- c. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f. The right to lodge a complaint with a supervisory authority;
- g. Where the personal data are not collected from the data subject, any available information as to their source;

h. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

### **Suitable Recitals**

(63) Right of access; (64) Identity verification.

### **COMMENTARY:**

The Regulation does not actually provide for anything new as to the right to access but accepts the principle contained in the Directive: the data subject shall have the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. Specific information must be given pursuant to the right of access. Compared to the previous system, new information elements are provided for, such as, in particular, the obligation to inform the data subject about the period of storage, of their right to rectification and erasure, of their right to lodge a complaint with a supervisory authority, of the specific safeguards taken in case of data transfer to a third country or an international organization or information on the existence of an automated decision including profiling.

If so requested, the data subject is entitled to be issued a copy of the data. Such copy must be free of charge because the final text provide for a payment of fees on the basis of the administrative costs of controller for the subsequent copies only. On the other hand, the text says nothing about the possible costs related to the access without a copy (while the previous version explicitly provided for the free access with no payment at regular intervals). The provision also states that the information may be provided electronically, unless otherwise requested, when the request for access was made electronically.

Finally, the final version of the Regulation stipulates in paragraph 4 that the right to obtain a copy must not adversely affect the rights and freedoms of others. In the previous version of the Regulation, an exception to the right to obtain a copy could be made if the issue of copies involved the disclosure of confidential data or

was likely to infringe intellectual property rights on processing. In its Article 12, the Directive already granted a broad right of access to e data to data subjects.

### **Section 3: Rectification and erasure**

#### **Art. 16 GDPR Right to rectification**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

#### **Suitable Recitals**

(65) Right of rectification and erasure.

#### **COMMENTARY:**

Under this Article individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data. Data subjects are entitled to require a controller to rectify any errors in their personal data. Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

Rectification may be requested when the name, address or any other information has been misspelled. Usually, the data subject will first request access in order to verify if the data has been indeed misspelled. If it has been, rectification should be made as soon as possible. Another scenario where rectification will be needed is the case when some information is changed – for example the home address. The time frame to address a rectification is one month. In case of complex and/or high volume requests the controller can seek an extension for up to two additional months.

Article 12 (b) of the Directive granted the data subjects the right to obtain, as appropriate, rectification, erasure or blocking of data, the processing of which does not comply with the Directive, in particular because of incomplete or inaccurate nature of the data. The right to rectification is intended to complement the right of access, giving to the data subject the power to prevent the processing activities from resulting in the distribution or use of false information.

#### **Art. 17 GDPR Right to erasure ('right to be forgotten')**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall



have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - b. The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
  - c. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
  - d. The personal data have been unlawfully processed;
  - e. The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
  - f. The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
- a. For exercising the right of freedom of expression and information;
  - b. For compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - c. For reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
  - d. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - e. For the establishment, exercise or defence of legal claims.

### **Suitable Recitals**

(65) Right of rectification and erasure; (66) Right to be forgotten.

### **COMMENTARY:**

Data subjects are entitled to require a controller to delete their personal data if the continued processing of those data is not justified. Data subjects have the right to erasure of personal data (the "right to be forgotten") if:

- The data are no longer needed for their original purpose (and no new lawful purpose exists);
- The lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- The data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- The data have been processed unlawfully; or
- Erasure is necessary for compliance with EU law or the national law of the relevant Member State.

Presented with great fanfare as the major innovation of the Regulation, the right to erasure, however, was already contained, at least in embryo in the Directive, in its Article 12, paragraph (b). We refer here to the important judgment delivered by the Grand Chamber of the Court of Justice of the European Union of 13 May 2014 ((CJEU, Google Spain SL c. Costeja, 13 May 2014, C-121/12). After considering that Google is subject to the provisions of Directive 95/46/EC (or the transposition law) and considered to be a data controller, the Court found that the right to rectification and to object enshrined in those provisions permit a person to remove links to data.

The requests under Articles 12 (b) (rectification) and 14, first paragraph, (a) (object) of the Directive could be made directly by the data subject to the controller who must duly consider the grounds thereof and, if necessary, terminate the processing of the data in question. When the controller fails to respond to these requests, the data subject can notify supervisory authority or judicial authority to carry out the necessary checks and order the controller to perform specific actions accordingly.

### **Art. 18 GDPR Right to restriction of processing**

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
  - a. The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
  - b. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - c. The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d. The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

### **Suitable Recitals**

(67) Restriction of processing.

### **COMMENTARY:**

In some circumstances, data subjects may not be entitled to require the controller to erase their personal data, but may be entitled to limit the purposes for which the controller can process those data (e.g., the exercise or defense of legal claims; protecting the rights of another person or entity; purposes that serve a substantial public interest; or such other purposes as the data subject may consent to). Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:

- The accuracy of the data is contested (and only for as long as it takes to verify that accuracy);
- The processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure);
- The controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or
- If verification of overriding grounds is pending, in the context of an erasure request.

Article 12 (b) of the Directive already required the Member States to ensure to the data subject the right to obtain blocking of data, the processing of which does not comply with the Directive, in particular because of incomplete or inaccurate nature of the data. The notion of "blocking of data" has not, however, been subject to any definition in the Directive.

### **Art. 19 GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing**

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1)

and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

### **Suitable Recitals**

(66) Right to be forgotten.

### **COMMENTARY:**

It is only possible to give full effect to the rights of data subjects if all parties who are processing the relevant data are aware that the data subject has exercised those rights. Therefore, controllers must notify any third parties with whom they have shared the relevant data that the data subject has exercised those rights.

Where a controller has disclosed personal data to any third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or blocking, the controller must notify those third parties of the data subject's exercising of those rights. The controller is exempt from this obligation if it is impossible or would require disproportionate effort. The data subject is also entitled to request information about the identities of those third parties. Where the controller has made the data public, and the data subject exercises these rights, the controller must take reasonable steps (taking costs into account) to inform third parties that the data subject has exercised those rights.

The Directive already required the states to guarantee to data subjects the right to obtain notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort (see Article 12 c)).

### **Art. 20 GDPR Right to data portability**

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

1. The processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

2. The processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

### **Suitable Recitals**

(68) Right of data portability.

### **COMMENTARY:**

This right applies if the processing is carried out by automated means and Data Subject provided personal data on the basis of his or her consent, or the processing is necessary for the performance of a contract. Under those conditions, if the Data Subject requests it: (i) provide with the data received by the DS in a structured, commonly used and machine-readable format and, (ii) allow the transmission of the data to another DC.

This new right is one of the major innovations of the Regulation and in general, probably expresses a very important development in the progress to recovery of control on the data by the data subject itself. If the goal is laudable, it remains to see how it will be implemented in practice, insofar as it implies a dialogue of the controllers and doubtlessly, an agreement - at least implicit - on the means and the standards used for data recovery. The text says nothing about the further use of the data by the first controller with which this right is exercised. It is concluded that the general principles of protection continue to apply and that the controller can keep it only to the extent strictly necessary for the announced purposes. The text says nothing either about the fate of the data "generated" by the use of a product or service and which are not actually 'communicated' by the data subject: data related to billing, traffic data, location data, etc. Are they covered by this new right?

## **Section 4: Right to object and automated individual decision making**

### **Art. 21 GDPR Right to object**

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

### **Suitable Recitals**

(69) Right to object; (70) Right to object to direct marketing.

### **COMMENTARY:**

According to Article 21 of the Regulation, the right to object may be exercised on grounds relating to the data subject's particular situation and for processing based on:

- Article 6 (1), e), i.e., “the processing is necessary to the performance of a task in the public interest or in the exercise of the official authority vested in the controller”;
- Article 6 (1), f), i.e., when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

It should be noted in extreme is that these assumptions included the profiling done on these grounds. In other words, the right to object, as it was initially provided for in the Directive, can be invoked in both cases of lawfulness of processing covered and not, for example, when the processing is based on the data subject's consent. While the Directive to the Member States provides at least the application of the right to object in these two cases of processing, the Regulation seems opposed to the extension of the scope of the right to object any further, as provided for in some national laws under the Directive.

This restriction seems to be partially compensated by the possibility to withdraw the consent to processing at any time, which will require the controller to refuse to continue the processing, knowing that the withdrawal of consent does not question the lawfulness of the processing prior to the withdrawal (Art. 7 (3)). Furthermore, the controller may refuse to implement the right to object of the data subject when

establishing the existence of compelling and legitimate grounds justifying the processing, which take priority over the data subject's interests or rights and freedoms, or for the recognition, exercise or defence of a legal right. The Regulation also provides that the data subject may object at any time the processing of their personal data for marketing purposes, including profiling done for this purpose (Art. 21 § 2).

The existence of these rights to object must be brought to the knowledge of the data subject, clearly and separately from any other information, at the time of the first communication with the data subject at the latest. The notification can be made by automated means as part of an offer of the use of an information society service and notwithstanding the Directive 2002/58/EC. Finally, the controller may refuse to proceed with the right to object of the data subject when the data are processed for historical, statistical or scientific purposes in the meaning of Article 89, if he or she can demonstrate that the processing is necessary for the performance of a task of public interest.

The right to object by the person concerned by a processing of personal data was already provided by Article 14 of the Directive. Such right allowed any person to object to the processing of his or her data, by referring to "compelling legitimate grounds relating to his particular situation", at least when the processing was necessary for the performance of a public controller (Article 7 (e)) or when the processing was based on the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed (Article 7 (f)). In addition, this right allowed anyone to object to the processing of his data for marketing purposes, regardless of the basis for processing.

## **Art. 22 GDPR Automated individual decision-making, including profiling**

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
  1. Is necessary for entering into, or performance of, a contract between the data subject and a data controller;
  2. Is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
  3. Is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(2)(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

### **Suitable Recitals**

(71) Profiling; (72) Guidance of the European Data Protection Board regarding profiling; (91) Necessity of a data protection impact assessment.

### **COMMENTARY:**

Article 15 of the Directive already recognized the right of individuals not to be subject to a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as their performance at work, creditworthiness, reliability, conduct, etc. However, exceptions were provided under conditions once the decision was taken as part of the conclusion or performance of a contract or was authorised by a law providing safeguards for the legitimate interest of the person.

Do not impose a decision based solely on automated means, including profiling, which produces legal effects concerning the Data Subject or similarly significantly affects him or her; unless, is necessary for entering into, or performance of a contract between the DC and Data Subject or is based Data Subject's explicit consent or is authorised by Union or Member State Law.

In any case, such a processing should be subject to suitable safeguards. Which should include at a minimum, the provision of specific information to the Data Subject, the right to obtain human intervention, to the possibility of the Data Subject to express his/her point of view, to obtain an explanation of the decision and to be able to challenge it. This measure should not concern a child.

## **Section 5: Restrictions**

### **Art. 23 GDPR Restrictions**

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- a. National security;
- b. Defense;
- c. Public security;



- d. The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
  - e. Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
  - f. The protection of judicial independence and judicial proceedings;
  - g. The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
  - h. A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
  - i. The protection of the data subject or the rights and freedoms of others;
  - j. The enforcement of civil law claims.
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
- a. The purposes of the processing or categories of processing;
  - b. The categories of personal data;
  - c. The scope of the restrictions introduced;
  - d. The safeguards to prevent abuse or unlawful access or transfer;
  - e. The specification of the controller or categories of controllers;
  - f. The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
  - g. The risks to the rights and freedoms of data subjects; and
  - h. The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

### **Suitable Recitals**

(73) Restrictions of rights and principles.

### **COMMENTARY:**

Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal

penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Under the Directive (Art. 13), the Member States were already allowed to limit the scope of the rights and obligations provided for in Article 6 on the quality of the data; in Articles 10 and 11 relating to the information to be provided to the data subject; Article 12 on the right to object and article 21 on the publicizing of processing. However such limitations are measures necessary for the implementation of exhaustively listed interests, for example, for ensuring the national security, defense, public security or prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics in the case of the regulated professions.

\*\*\*

## CHAPTER 4: CONTROLLER AND PROCESSOR

### Section 1: General obligations

#### Art. 24 GDPR Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

#### Suitable Recitals

(74) Responsibility and liability of the controller; (75) Risks to the rights and freedoms of natural persons; (76) Risk assessment; (77) Risk assessment guidelines.

#### COMMENTARY:

##### Controller

The term of controller is under both frameworks from high importance, the party who is considered to be controller is responsible for ensuring compliance with the law.

The DPD defines controller in Art.2(d) as: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws. The definition is divided in the elements “determines”, “purposes and means of processing” and “natural person, legal person or any other body” and “alone or jointly with others”. “Determines” shall stem from the factual elements of the circumstances of the case. The questions needed to be asked, to find out if somebody “determines” are: who sets the purposes?, If processing is taking place?, Who initiated it?

In the element of “purposes and means of processing” the dictionary defines purpose as the intended or desired result, aim, or the reason why something exists. The purpose is the “why” and “how” of processing. Whereas the two remaining elements are self-explaining “natural person, legal person or any other body” and “alone or jointly with others”. Art.4(7) of the GDPR defines controller as: the natural

or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller or the criteria for nominating the controller may be designated by those laws. Except from the part “or the criteria for nominating the controller” the definition is the same. Every entity considered to be a controller under the DPD is likely to be controller under the GDPR.

### **Controller`s obligations**

The fact that a party is considered to be controller is connected to a list of obligations, which characterise the controller-status. The principle of accountability is ought to ensure the enforcement of the main data protection principles. Under the Directive, Art.6(2) only the controller is accountable. He must ensure compliance with the main data protection principles, when processing. Whereas under the GDPR the controller is not only accountable, but must also be able to demonstrate compliance with the main data protection principles, Art.5(2), rec.85.

The measures to demonstrate compliance have to be “appropriate technical and organizational measures” and codes of conduct, Art.24 GDPR. The GDPR tries to set down criteria in rec.74 GDPR to determine what a appropriate measure could be. The controller should take into account the nature, scope, context and risk to the rights and freedoms of natural persons.

Article 24 is implementing a "general principle of responsibility" at the forefront of the general obligations of the controller, the definition of which remains unchanged since the Directive (see G29, Opinion 3/2010 of 13 July 2010, on the principle of responsibility). Actually, the controller is defined as: “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes (...) and the means of the processing of personal data” (Art. 4 (7)).

The principle included in the first paragraph is divided into two rules. The *first rule* confirms the special responsibility of the controller in the implementation of the appropriate technical and organizational measures to perform the processing in accordance with the Regulation.

The initial proposed version provided for a list of the measures in question, but this has not been included in the final version. However, the list is very useful to understand the scope of the principle. The version covered most of the unspecified general measures or a bit specified by the text of the Regulation, such as: maintaining of the documentation provided for in Article 30, the implementation of the obligations of data security provided for in Article 32, conducting an impact assessment on the protection of data in application of Article 35, the compliance with the obligations of authorization or preliminary consultation of the supervising authority in application of Article 36 (1) and (2), the designation of a data protection officer in application of article 37 (2) and (3).

This first rule also provides that to determine the appropriate technical and organizational measures, account must be taken of the nature, the scope, the context and the purpose of processing as well as the likelihood and the severity of risks with respect to the rights and freedoms of natural persons.

Recitals 75 and 76 give many examples of the envisaged risks: processing that is likely to result in physical, material or moral damage, in particular when the processing may give rise to discrimination, an identity theft or usurpation, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy, when it comes to processing of sensitive data, when personal aspects are evaluated, etc. The probability and the severity have to be assessed depending on the nature, the scope, the context and the purpose of the processing of data. The risk should be subject to an objective assessment to determine if the data processing operations carry a high risk. According to recital 60 (3), high risk means a particular risk of prejudice to the rights and freedoms of individuals.

Paragraph 2 of Article 24 says that where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. The *second rule* stems from the first and is focused on the proof of the implementation of these measures. Then, the burden of proof rests on the shoulders of the controller which must be able to demonstrate that the personal data is processed in compliance with the Regulation.

The third paragraph provides that adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller. Recital 77 (4) includes the indications given by the data protection officer.

Neither the Directive nor the legislation analysed in this commentary provided a provision comparable to that provided for in Article 22 of the Regulation.

## **Art. 25 GDPR Data protection by design and by default**

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as Pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for

each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

### **Suitable Recitals**

(78) Appropriate technical and organisational measures.

### **COMMENTARY:**

**“Design is a funny word. Some people think design is how it looks. But of course, if you dig deeper, it’s really how it works.” -Steve Jobs**

The EU Data Protection Directive did not explicitly include privacy by design. However, given that the right to privacy is a fundamental element of the European Convention on Human Rights, it was clear that those designing technology ought to consider privacy as part of their product design, in the same way that they would take measures to not discriminate on the basis of race or gender as part of that process. The formalisation of that position is therefore included in the GDPR.

The principle of privacy by design and by default is consistent with, and an extension of, the requirement for data minimisation under Article 5 of the GDPR; namely that systems and technology should be designed in such a way so as to ensure that: (i) data processing is limited to what is necessary for the purpose for which the data was collected; and, (ii) only those within an organisation who need to access the personal data can do so.

The GDPR provides for a voluntary certification by which entities can demonstrate compliance with the principles of design and default by way of data protection seals and marks. Given that the privacy rights that the GDPR promotes are likely to change the expectations of citizens, when considering future products, such a proposal provides for a commercial advantage to those that choose to obtain these seals and marks, rather than just a regulatory obligation - again furthering the principle that the subjects are champions of the data.

The GDPR obliges controllers to implement measures of safeguard in every planning or processing phase of every new product or service, Art.25, rec.78.

### **Compliance Description**

Article 25 conveys the key principles—privacy by design and privacy by default—underlying the entire GDPR. For example:

- Article 5 (1) requires that data processing be limited to what is necessary given the purpose for which the data is initially collected (privacy by design) and be limited to those who need to access the data (privacy by default).

- Article 32 (1) (b) requires the ongoing confidentiality and integrity of processing data processing systems and services (data privacy by design and default).

Although, Pseudonymisation and data minimization are required technical measures, Article 25 gives Data Controllers flexibility in determining which additional technical measures best ensure data security and privacy. When selecting a measure, the Data Controller must document an evaluation of the measure along four criteria:

- **State of the Art:** An evaluation of the latest and most advanced data security and privacy enhancement tools available. For example, some newer technologies are *behavior analytics* that profile normal behavior patterns and trigger alerts when a divergence occurs, *privileged user monitoring* that checks user activities and blocks access to data if necessary, and *Format Preserving Encryption* (FPE) that encrypts data employing the existing database format.
- **Processing Profile:** An evaluation of the nature, scope, context, and purposes of the data processing.
- **Risk Profile:** An evaluation of the likelihood and severity of risks to the rights and freedoms of natural person when processing personal data. Risks include “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processes.” Conducting a risk assessment is best done with a Privacy Impact Assessment (PIA), as specified in Article 35 of the GPDR.
- **Cost:** An evaluation of the cost of implementation relative to the risk profile.

Data privacy by design ensures that privacy is built into products, services, application, business and technical processes. Data privacy by default protects a natural person’s fundamental rights and freedom to protection of their personal data. Implementing data privacy by design and default guarantees, at a minimum, that:

- Only personal data necessary for a specific purpose is collected.
- Only data relevant to the original data collection purpose can be processed.
- Data that is no longer needed must be deleted.
- Natural persons can opt in or opt out of any collection, storage, processing, or deletion of their personal data.

## **Compliance Methods**

Complying with Article 25 requires both organizational and technology strategies.

### **Organizational Strategies**

A few organizational strategies are:

- Not copying production databases for development, testing, or analytics purposes. Instead the data should be anonymized or pseudonymized.

- Not storing spreadsheets and other data sources in a local folder or to a SaaS application such as Box, Dropbox, Google Drive, or OneDrive.
- Limiting email archive access to a limited number of privileged users and monitoring their activity.
- Requiring encryption of emails containing identifiable personal data.
- Protecting personal data at-rest, in-motion, and in-use employing an existing database format.
- Setting and enforcing policies about using bring-your-own-devices to access secured data.
- Implementing staff training, internal audits of processing activities, policy reviews, and documentation of compliance

### **Technology Strategies**

Ensuring data privacy by design and default can be achieved through:

- Data masking: Anonymizes data via encryption/hashing, generalization, perturbation, etc. Pseudonymizes data by replacing sensitive data with realistic fictional data that maintains operational and statistical accuracy.
- Ethical walls: Maintains strict separation between business groups to comply with M&A requirements, government clearance, etc.
- Privileged user monitoring: Monitors privileged user database access and activities. Blocks access or activity, if necessary.
- User rights management: Identifies excessive, inappropriate, and unused privileges.
- User tracking: Maps the web application end user to the shared application/database user to the final data accessed.
- VIP data privacy: Maintains strict access control on highly sensitive data, including data stored in multi-tier enterprise applications such as SAP and PeopleSoft.

### **Art. 26 GDPR Joint controllers**

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.



2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

### **Suitable Recitals**

(79) Allocation of the responsibilities.

### **COMMENTARY:**

The definitions of the controller allowed, as the Directive did, to qualify as "joint controllers" several people who jointly define the purposes and the means of the processing (see Article 2, d)) of the Directive.

### **Joint controllers and their obligations**

Where two or more controllers determine the purposes and means of processing, they are joint controllers (Article 26). Under the GDPR joint controllers have to determine their respective responsibilities for legal compliance and rights of data subjects in a transparent manner. They can do so for example in a clear contractual arrangement. The arrangement needs to reflect the roles and relationships between the joint controllers and made available to data subjects. A data subject may exercise his or her rights against each of the controllers. Each data controller is individually liable for legal compliance under Article 82. After providing remedies to data subjects, a joint controller may claim its losses from other joint controllers or processors, if applicable, according to its roles and responsibilities in the processing at stake.

Under the term joint data controllers GDPR has a specific set of requirements, as defined under Article 26 – Joint Controllers. Under GDPR, the term joint data controllers is defined as “where two or more controllers jointly determine the purposes and means of processing”. But in what scenarios would joint data controllers be defined? And how can we identify these? This article looks at joint data controllers GDPR defines in more detail.

Within the definition for joint controllers GDPR states that two or controllers may act as joint data controllers where each party has responsibility, or shared liability, for the data in question. The Article 29 working party guidance expands on this to state that where controllers are acting simultaneously on personal data to provide a service to a consumer this may also result in a joint data controller. For example, if data is collected through a web front end and provided to 2 separate entities who conduct some form of processing, but are ultimately responsible for the security of said data, this may result in joint data controllers. While there is no definitive list of where joint data controllers should be used, it is more often than not when both parties have clear obligations, and liabilities, to the data subjects that joint data controllers should be used.

Joint data controllers by their nature work together to determine how personal data should be processed, and the manner of processing. To confuse matters, the term data controllers in common can be used to describe where two controllers are processing data independent of each other. So using the example provided above, were both entities to jointly decide how to protect and manage personal data collected, they would be joint data controllers. If both parties were independently processing said data, with no arrangements or agreements between each other, then both parties would be data controllers in common.

Why is it so important under GDPR? Well, the obligations for controllers and processors vary. Therefore, it is imperative organisations understand their role with regards to personal data. Joint data controllers must be identified and relationships established so both parties are happy with how data is processed, whereas controllers in common have little interest in how the other party is processing this data, as they are no longer liable for it under GDPR. So for joint data controllers GDPR requires that each party clearly define their responsibilities under the regulation. For example, how would data subject rights be managed between both parties e.g. right to erasure or subject access requests? And how about in situations where one party has differing requirements, how is this communicated and agreed?

The answer is that specific arrangements need to be drawn up where joint data controllers are identified. The term agreement and not contract is key here, it is not mandatory under GDPR to have contracts in place between joint data controllers, although an agreement should be in place that ensures clarity between both parties. Agreements should be drawn up, agreed by both parties and monitored over time as per any contract or agreement with a third party.

The key point is that joint data controllers GDPR requirements are relatively unclear, and it is left to the organisation to identify scenarios where they feel joint data controllers are needed. When those situations arise, both controllers should be clear on what their responsibilities are, and how they will comply with managing personal data securely in a joined up manner.

### **To summaries:**

1. Joint data controllers are both responsible for determining the processing requirements for personal data under their control.
2. Joint data controllers are not the same as data controllers in common, who process the same data in different ways. There is no requirement for alignment or agreements to be in place for controllers in common.
3. Agreements should be in place between joint data controllers which set out the roles and responsibilities for both parties. This does not need to be a contract but should be clear, unambiguous and regularly monitored/reviewed.
4. Joint data controllers GDPR definitions are not prescriptive. Article 26 only specifies a minimal amount of information so do not under estimate the amount of

work that may be required to determine where joint data controllers may be required.

5. Establish use cases for joint data controllers and ensure that any new projects, systems or joint ventures, for example, consider that joint data controller agreements may be required.

Under the Directive, joint controllers are generally only liable for the harm for which they are responsible. This means that, in some circumstances (e.g., where one of the joint controllers becomes insolvent) data subjects may not be able to obtain full compensation for any harm arising from the joint processing. The GDPR reverses this approach, making each of the joint controllers fully liable to the data subject. The data subject is therefore entitled to bring a claim against whichever of the joint controllers he or she wishes. Once "full compensation" (a term that is not further explained in the GDPR) has been paid, the joint controller(s) who paid that compensation may then seek to recover damages from any other joint controllers involved in the joint processing. There is an exemption, but it only applies if the controller is not in any way responsible for the harm. Consequently, where a joint controller only has minimal responsibility for that harm, it nevertheless remains liable to pay "full compensation" to affected data subjects. It is likely that, under the GDPR, joint controllers will increasingly seek contractual indemnities from one another prior to commencing any joint processing.

#### **Art. 27 GDPR Representatives of controllers or processors not established in the Union**

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

1. processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

2. a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions, which could be initiated against the controller or the processor themselves.

### **Suitable Recitals**

(80) Designation of a representative

### **COMMENTARY:**

In the case of application of Article 3 (2), Article 27 of the Regulation requires the controllers and the processors who are not established in the Union to designate in writing a representative, when the Regulation applies to their processing activities. As explained above (see Comment to Article 3.2), the Regulation was made applicable to a controller or a processor who is not established in the Union, where the processing activities are related to the supply of goods or services to such data subjects in the Union, a payment is required or not from such data subjects or to the monitoring of their behaviour, to the extent that it takes place within the European Union.

Let us recall that pursuant to Article 4 (17) of the Regulation, the representative is "a natural or legal person established in the Union designated by the controller or processor in writing pursuant to Article 27 who represents the controller or processor with regard to their respective obligations under this Regulation". Let's note again that a written agreement is required for such designation.

The provision specifies that this obligation does not apply to processing that is occasional and that does not include, on a large scale, the processing of sensitive data within the meaning of Article 9 (1) or data on convictions and criminal offenses (Art. 10) and is not likely to create risk to the rights and freedoms of natural persons, taking into account the processing nature, context, scope and purposes. This applies even when the controller or the processor is an authority or a public body.

This representative must be established in one of the Member States in which reside the natural persons whose personal data are processed in the context of the supply of goods or services they are offered or whose behaviour is monitored.

The representative, who acts on behalf of the controller or the processor, is namely the point of contact for the supervisory authorities (see Article 58) and the data subjects on all matters relating to the processing of personal data. The representative must be expressly authorised in writing by the controller or the processor to act on their behalf to fulfill their duties under the Regulation and to be consulted in addition to or instead of the controller or the processor, including the supervisory authorities and the data subjects.

This representative is also required to maintain a register of all types of personal data processing activities carried out under their responsibility (see Article 30). The main innovation of the second draft Regulation is to provide the possibility of imposing coercive measures against the representative in case of non-compliance

with this Regulation by the controller (see recital 80 and Article 27 (4) of the Regulation). However, the designation of a representative does not affect the responsibility of the controller or the processor in respect of the authorities and the data subjects, since the designation of a representative is without prejudice to the legal actions could be brought against the controller and the processor themselves. Article 4.2. of the Directive provided that the controller who has no establishment in the EU but which falls under the Union law under the extraterritorial criteria for application of European regulations must designate a representative in the territory of the member State having jurisdiction under Article 4.1. c).

## **Art. 28 GDPR Processor**

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

- a. Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- b. Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- c. Takes all measures required pursuant to Article 32;
- d. Respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- e. Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for

the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f. Assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g. At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h. Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3. shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

### **Suitable Recitals**

(81) The use of processors.

### **COMMENTARY:**

Article 4 (8) defines the processor using the definition already available in the Directive. The processor is: “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. Article 28 of the Regulation extends the previous duties of controllers and processors while organizing a separate regime for their duties for security referred to in Article 32 et seq.

As before, the controller can only choose contractors with sufficient safeguards with respect to taking of appropriate technical and operational measures to meet the requirements of the Regulation and to ensure protection of the rights of the data subject.

The principle is still that of a specific contract between the controller and the processor, or by another specific legal act provided for the needs of the Union or of a Member State, binding the subcontractor and the controller. On the other hand, the content of the written contract - including an electronically format is extended. In addition to information on the processing itself (purpose, scope and duration of processing, etc.), the contract provides for the commitment of the processor to comply with a range of duties *vis-à-vis* to the controller, namely:

- to process the personal data only on documented instructions from the controller – which was already provided – but these instructions will now be specifically documented - in particular the transfers of data to third countries – by the controller. An exception is made for the legal duties, which would subject the contractor who will be the subject of specific information by the processor, except for a justified legal exception for important reasons of public interest;

This duty is also reflected in Article 32 requiring the controller to take measures to ensure that anyone who has access to data under the authority of the controller or the processor can process them only on their instructions, unless required to do so by the law of a member State or a rule of the EU and provided that they inform the controller accordingly, unless such information is prohibited for important reasons of public interest.

- To ensure that persons authorised to process the personal data have committed themselves to confidentiality;

- To respect the conditions referred to in paragraphs 2 and 4 for engaging another processor (see below);
- To assist the controller for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights;
- To assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the Regulation;
- At the choice of the controller, to delete or return all the personal data to the controller after the end of the provision of services;
- To make available to the controller all information necessary to demonstrate compliance with Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Article 28 also requires the processor to immediately report to the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. In addition to the duties provided for by the Directive, the Regulation organizes the question of processing entrusted to third parties - secondary processors by the direct processor of the processing controller, very common cases in practice. Thus, the possibility left to the secondary processor of the processor itself will be subject to a prior written consent (specific or general) by the controller. In the case of a written general authorization, the direct processor must inform the controller, prior to any change of the "secondary" processor to enable the controller to object.

In addition, this secondary processor contract must comply with the rules applicable to the content of the contract entered into between the controller and the main processor (Art. 28 (4)). Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which the processor shall demonstrate sufficient guarantees. The Regulation expressly provides the possibility of using standard contractual clauses provided by various sources as the basis of the specific contract between the controller and the processor (included in a procedure of certification, of the Commission or the supervisory authorities). The Commission is also empowered to establish standard contractual clauses for the matters referred to in paragraphs 3 and 4, in accordance with the consistency mechanism referred to in Article 63.

Finally, the last version of the Regulation specifically indicates that if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing. Article 17 of the Directive organized the system of processors as part of the security obligations. The Directive provided that the controller who acts through a processor



should ensure that such processor provides sufficient guarantees as to the implementation and the compliance with the security measures to be implemented. A binding legal contract or act should bind the controller and the processor, the latter having to state in particular that he or she will act only on instructions from the controller, as well as the safety measures he or she had to take.

### **Art. 29 GDPR Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

#### **COMMENTARY:**

Article 16 of the Directive established the fundamental principle of confidentiality with respect to the personal data protection: any activity dealing with personal data processing can be performed only on the instruction of the controller. This requirement also applies to any person who has access to the personal data, whether this access is made by a person acting under the authority of the controller or the processor as well as to the processor him/herself.

### **Art. 30 GDPR Records of processing activities**

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- a. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- b. The purposes of the processing;
- c. A description of the categories of data subjects and of the categories of personal data;
- d. The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- e. Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- f. Where possible, the envisaged time limits for erasure of the different categories of data;
- g. Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- a. The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- b. The categories of processing carried out on behalf of each controller;
- c. Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- d. Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

### **Suitable Recitals**

(13) Taking account of micro, small and medium-sized enterprises; (82) Record of processing activities.

### **COMMENTARY:**

A data processing inventory reflects how the business processes data and starts with listing the processing activities and their purpose. A data processing inventory is aligned with how the business works, making it is easy for the business to engage. The GDPR creates an opportunity for organizations to limit their data inventory. Organizations need an inventory of their data processing operations, instead of all their data holdings and detailed inventory.

It is worth taking the time and effort to document each processing activity at the individual processing activity level. For example, 'how do we pay employee wages', 'how does someone register with our site', 'how does someone enter a competition'. Bear in mind that the same data sets, or components of the same data sets, might have multiple processing activities. Someone buying a product from an online ecommerce store will have their data processed to fulfill and deliver the

product. They might also have their personal data processed by a CRM team for marketing purposes, as well as by your finance team for statutory accounting activity.

When gathering this data, consider completing the following fields in a template that we can provide to you (this template also helps you analyze the data to produce useful metrics)

- Legal entity and department;
- Process owner;
- Step by step process flow – from collection to disposal;
- Categories of data collected;
- Data subjects (e.g., employees, customers);
- Lawful grounds for processing;
- Volumes of data;
- Where data is stored (location);
- Where there is an European Economic Area transfer, what is the legal mechanism for this;
- Retention period (or to agree on retention periods where they have not yet been decided);
- Who has access to the data;
- Are there any data processors involved in the process (and who they are);

If so, has information security due diligence been conducted;

- Check of the contract clauses to see if they meet Article 28 (Processor) requirements;
- Notes on security measures applied.
- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.

- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

For organisations operating in the EU, a requirement of the EU Data Protection Directive 95/46/EC was to notify and register processing activities with local DPAs. Article 30 replaces this requirement and in this context, a processing data inventory is the same as a “records of processing activities” register. It is important to note this list is first concerned with the details of processing activities versus the details of a data holding repository and does not require the onerous process of documenting every data element that forms part of the data repository (though in practice, some companies may still want to do this).

Under the Directive, Article 16 (2) authorised the Member States to provide for two exceptions to the obligation to send a notification to the supervisory authority prior to the implementation of any processing:

- The first one covered the categories of processing that are not likely to infringe the rights and the freedoms of the data subjects, given the data to process and as long as they specify the purposes, the categories of processed data, the data subjects, the recipients and the period of storage;
- The second one aimed at the assumption where the controller has designated a seconded data protection officer charged, on the one hand, to ensure the compliance of the data protection legislation and on the other hand, to maintain records of the processing activities.

### **Art. 31 GDPR Cooperation with the supervisory authority**

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

#### **Suitable Recitals**

(82) Record of processing activities.

#### **COMMENTARY:**

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

Article 31 GDPR stipulates the general obligations to cooperate with supervisory authorities. This obligation applies to the controller, processor and if applicable their respective representatives. The important is corporation shall take place at the

request of the supervisory authority, the controller and the processor does not have to cooperate on its own.

## **Section 2: Security of personal data**

### **Art. 32 GDPR Security of processing**

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- a. The Pseudonymisation and encryption of personal data;
- b. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- c. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

### **Suitable Recitals**

(75) Risks to the rights and freedoms of natural persons; (76) Risk assessment; (77) Risk assessment guidelines; (78) Appropriate technical and organisational measures; (79) Allocation of the responsibilities; (83) Security of processing.

### **COMMENTARY:**

Article 32 of the General Data Protection Regulation (GDPR) requires Data Controllers and Data Processors to implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data. In addition, Article 32 specifies that the Data

Controller or Data Processor must take steps to ensure that any natural person with access to personal data does not process the data except on instruction of the controller, processor, European Union law, or member state law. Compliance with Article 32 requirements can be demonstrated by adherence to an approved code of conduct as specified in Article 40 or an approved certification as specified in Article 42.

### **Compliance Description**

Data security measures should, at a minimum, allow:

- Pseudonymisation or encrypting personal data.
- Maintaining ongoing confidentiality, integrity, availability, access, and resilience of processing systems and services.
- Restoring the availability of and access to personal data, in the event of a physical or technical security breach.
- Testing and evaluating the effectiveness of technical and organization measures.

Although Pseudonymisation and encryption are required technical measures, Article 32 gives Data Controllers flexibility in determining which additional technical measures best ensure data security. However, when selecting a measure, the Data Controller must document an evaluation of the measure along four criteria:

- **State of the Art:** An evaluation of the latest and most advanced data security and privacy enhancement tools available. For example, some newer technologies are *behavior analytics* that profile normal behavior patterns and trigger alerts when a divergence occurs, *privileged user monitoring* that checks user activities and blocks access to data if necessary, and *Format Preserving Encryption* (FPE) that encrypts data employing the existing database format.
- **Processing Profile:** An evaluation of the nature, scope, context, and purposes of the data processing.
- **Risk Profile:** An evaluation of the likelihood and severity of risks to the rights and freedoms of natural person when processing personal data. Risks include “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processes.” Conducting a risk assessment is best done with a Privacy Impact Assessment (PIA), as specified in Article 35 of the GPDR.
- **Cost:** An evaluation of the cost of implementation relative to the risk profile.

### **Compliance Methods**

Complying with Article 32 requires both organizational and technical strategies. Organizational strategies are similar to those specified for Article 25 compliance. Technical strategies include:

- **Change management:** Monitors, logs, and reports on data structure changes. Shows compliance auditors that changes to the database can be traced to accepted change tickets.
- **Data discovery and classification:** Discovers and provides visibility into the location, volume, and context of data on premises, in the cloud, and in legacy databases. Classifies the discovered data according to its personal information data type (credit card number, email address, medical records, etc.) and its security risk level.
- **Data loss prevention:** Monitors and protects data in motion on networks, at rest in data storage, or in use on endpoint devices. Blocks attacks, privilege abuse, unauthorized access, malicious web requests, and unusual activity to prevent data theft.
- **Data masking:** Anonymizes data via encryption/hashing, generalization, perturbation, etc. Pseudonymizes data by replacing sensitive data with realistic fictional data that maintains operational and statistical accuracy.
- **Data protection:** Ensures data integrity and confidentiality through change control reconciliation, data-across-borders controls, query whitelisting, etc.
- **Ethical walls:** Maintains strict separation between business groups to comply with M&A requirements, government clearance, etc.
- **Privileged user monitoring:** Monitors privileged user database access and activities. Blocks access or activity, if necessary.
- **Secure audit trail archiving:** Secures the audit trail from tampering, modification, or deletion, and provides forensic visibility.
- **Sensitive data access auditing:** Monitors access to and changes of data protected by law, compliance regulations, and contractual agreements. Triggers alarms for unauthorized access or changes. Creates an audit trail for forensics.
- **User rights management:** Identifies excessive, inappropriate, and unused privileges.
- **User tracking:** Maps the web application end user to the shared application/database user to the final data accessed.
- **VIP data privacy:** Maintains strict access control on highly sensitive data, including data stored in multi-tier enterprise applications such as SAP and PeopleSoft.

### **Using the Latest Available Tools and Software**

According to Article 32 of the GDPR regulations, only the most recent technology will suffice when implementing appropriate technical and organizational measures. What this means is that you are required to use the newest tools and methods in order to secure customer data. Depending on the context, this can range from modern, up-to-date security tools, like web vulnerability scanners and tools for

logging and monitoring, to regular staff training and strong password policies. Databases servers, web servers and any other type of server software used in the organization have to be up-to-date and regularly patched in order to adhere to this part of the GDPR.

### **Handling and Processing Personal Data**

The nature, scope and purpose of the data processing an organization performs also needs to be documented. Data must also be stored appropriately. For example, credit card data has to be handled one way, whereas email addresses will be handled a different way. Generally, the rule is that it's best to store the minimum amount data possible in order to perform a specified task.

### **Segregating Data**

As an application of the above rule, organizations have to make sure they adjust their security measures to match the probability and severity of a breach against the potential impacts on rights and freedoms of data subjects. This means that a breach of websites that allow the exchange of sensitive data between journalists and sources, may have a higher impact on the rights and freedoms of the affected users than the breach of a site that allows people to share cooking recipes, for example. It's vital to separate and estimate these varying risks and then apply security measures appropriate to the risk.

### **Minimum Compliance Requirements in Article 32**

Article 32 of the GDPR regulations state that the minimum consequences arising from regulations should include the following:

- Personal data should be pseudonymised (for example, by replacing names with unique identifiers) and encrypted where possible.
- Ongoing confidentiality, integrity, availability and resilience of processing systems and services must be ensured. In other words, all data should be readily available to users, and provisions should be made to ensure that it is not read or tampered with by unauthorized persons, whether accidentally or on purpose.
- In case of a detrimental physical or technical incident, access to personal data must be able to be restored quickly. This refers to offsite backups and emergency strategies in case of unforeseen events.
- Organizations must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures that are designed to ensure the security of processing. In other words, organizations shouldn't blindly rely on established security measures, but proactively test them in order to see whether or not they work as intended. In the case of web applications, this would include penetration testing and regular application vulnerability scanning.



## **Consider All the Risks of Processing Data**

Article 32 further states that organizations must consider the risks that are presented by processing personal data. These risks might take the form of accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data. It also includes how personal data is accessed, transmitted and stored. This GDPR section closes by reiterating that only authorized persons should process data when they are required or instructed to do so. In summary, organizations should make sure that all personal data is safely stored and only transmitted to trusted, authorized persons and third parties.

## **The Road to GDPR Compliance**

Implementing the varying aspects of the GDPR regulations remains a challenge for many organizations. To help you get started we have written a white paper, *The Road to GDPR Compliance* – a high level overview of what organizations should do in order to become GDPR compliant.

## **Art. 33 GDPR Notification of a personal data breach to the supervisory authority**

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
  - a. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - b. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - c. Describe the likely consequences of the personal data breach;
  - d. Describe the measures taken or propose to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

### **Suitable Recitals**

(85) Notification obligation of breaches to the supervisory authority; (87) Promptness of reporting / notification; (88) Format and procedures of the notification.

### **COMMENTARY:**

Article 33 of the Regulation generalizes the obligation of notification of data breaches to the supervisory authority by specifying it (see also G29, Opinion 03/2014 of 25 March 2014, on the notification of personal data breaches). Pursuant to Article 33 (1), any personal data breach, as defined in Article 4 (12 of the Regulation, i.e., “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” must be notified to the supervisory authority as a rule.

In the second proposed version of the Regulation, only data breach that are likely to expose individuals to risk in terms of their rights and freedoms were covered by the obligation of notification to the supervisory authority. Examples were contained in Article 33 (1): discrimination, identity theft or impersonation, financial loss, unauthorised reversal of the Pseudonymisation, loss of reputation, loss of confidentiality of data protected by the professional secrecy or any other significant economic or social damage.

In its latest version, the rule is reversed: any breach of data must be subject to a notification unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The regulation also sets the time limits for notification, as the controller knows the breach. The notification must be made without unjustified delay and, if possible not later than 72 after the controller having become aware of the breach. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach. The minimum content of the notification - part of which may be deferred (without undue delay, see Art. 33 (4) is also set by the provision:

- Description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned (Art. 33 (3), a));
- The name and contact details of the data protection officer or other contact point (Article 33 (3), b));

- Description of the likely consequences of the personal data breach (Article 33 (3), c));
- Description of the measures taken or propose to be taken by the controller to address the personal data breach (Article 33 (3), d)).

Finally, the controller must keep track of each breach indicating its context, its effects and the measures taken to remedy. This documentation will enable the supervisory authority to check compliance with Article 33.

The Directive did not provide for an obligation of notification in the event of a personal data breach. On the other hand, a notification mechanism had been set up by the Directive 2002/58/EC on privacy and electronic communications, included into the Regulation No. 611/2013 on measures relating to the notification of personal data breaches.

#### **Art. 34 GDPR Communication of a personal data breach to the data subject**

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
  1. The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
  2. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
  3. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
  4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

## Suitable Recitals

(86) Notification of data subjects in case of data breaches; (87) Promptness of reporting / notification; (88) Format and procedures of the notification.

### COMMENTARY:

Unlike the notification to the supervisory authority (see Article 33), the final version of the Regulation only requires the controller to notify the data subject of data breaches that are likely to expose individuals to a high risk to their rights and freedoms.

Article 34 also defines the content of the notification to the data subject, which is also very close to the notification under Article 33, to which it is largely referred (see Art. 34 (2)). The final version of the regulation states that the communication must be made in a clear and simple language.

The period is a bit different from the notification to the supervisory authority since Article 34 (1) *in fine* indicates only that it must be done "without undue delay". The idea is that data subjects should without delay take any measures that are necessary to stop or mitigate the negative effects that may arise from the data breach (see recital 85). Article 34 (3) provides, however, for various exceptions to the notification to the data subjects.

- If the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption (a);
- Or if the controller has taken subsequent measures, which ensure that the high risk to the rights and freedoms of data subjects referred to in, paragraph 1 is no longer likely to materialize (b);
- Or it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (c).

Initially, according to the second proposed version of the Regulation, the notification was not necessary if it would create risk to affect an important public interest. This exception that, in our opinion, allowed a too large space for maneuvering to the controller was, however, removed in the final version of the Regulation. Ultimately, the final version of the Regulation adds a fourth paragraph to Article 34 granting to the supervisory authority the power to require the controller to notify the data subjects, taking into account the likelihood for the breach to result in a high risk for them. This provision also recognizes to the supervisory authority the power to evaluate whether the notification to the data subject is necessary, in view of the exceptions provided for in Article 34 (3) of the Regulation.

The Directive did not provide for an obligation of notification in the event of a personal data breach. On the contrary, the system set up by the Directive

2002/58/EC on privacy and electronic communications, included in Regulation No. 611/2013 on measures relating to the notification of personal data breaches.

A data controller must notify the competent supervisory authority of a personal data breach without undue delay and where feasible not less than 72 hours after the data controller becomes aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Art. 33(1).

When a data controller assesses the risk that is likely to result from a breach, the data controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. As noted in the Guidelines, the European Union Agency for Network and Information Security (ENISA) has issued recommendations for a methodology of assessing the severity of a breach, which data controllers and data processors may find useful when designing their breach management response plans. The data controller should consider the following criteria when assessing the risk to individuals as a result of a breach:

- The type of breach that has occurred;
- The nature, sensitivity and volume of personal data;
- The ease of identification of individuals;
- The severity of consequences for individuals;
- Special characteristics of the individual;
- Special characteristics of the data controller; and
- The number of affected individuals.

In the first notification, the data controller should inform the supervisory authority if the data controller does not have all the information required for reporting and subsequently will provide more details. Art. 33(4). If it is not possible to provide the information required for reporting at the same time, the information may be provided in phases without undue further delay. Id.

When the notification by the data controller to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay, which is permissible if the data controller provides reasons for the delay. However, delayed notification should not be viewed as something that regularly takes place.

The information required for reporting includes the name and contact details of the data protection officer or other contact point where more information can be obtained and a description of:

- The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and of personal data records concerned;
- The likely consequences of the personal data breach; and

- The measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Art. 33(3). In certain circumstances, where justified, and on the advice of law enforcement authorities, the data controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time. Recital 88.

A data controller must communicate the personal data breach to the data subjects without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons and the data controller has not either:

- Implemented appropriate technical and organizational protection measures which were applied to the personal data affected by the personal data breach and render the personal data unintelligible to any person who is not authorized to access it (e.g., encryption) or
- Taken subsequent measures, which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize. Art. 34(1) and Art. 34(3). Where such communication of the personal data breach to the data subjects would involve disproportionate effort, there instead shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
- The communication must describe in clear and plain language the nature of the personal data breach and include the name and contact details of the data protection officer or other contact point where more information can be obtained and a description of:
- The likely consequences of the personal data breach; and
- The measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Art. 34(2) and Art. 33(3).

There is a high risk to the rights and freedoms of individuals where the breach may lead to physical, material or non-material damage for individuals whose data have been breached and such damage includes discrimination, identity theft or fraud, financial loss, damage to reputation, loss of control over personal data or limitation of rights, unauthorized reversal of Pseudonymisation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

### **Section 3: Data protection impact assessment and prior consultation**

#### **Art. 35 GDPR Data protection impact assessments**

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
  - a. A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - b. Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
  - c. A systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations, which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
7. The assessment shall contain at least:
  - a. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
  - b. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
  - c. An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

### **Suitable Recitals**

(75) Risks to the rights and freedoms of natural persons; (84) Risk evaluation and impact assessment; (89) Elimination of the general reporting requirement; (90) Data protection impact assessment; (91) Necessity of a data protection impact assessment; (92) Broader data protection impact assessment; (93) Data protection impact assessment at authorities.

### **COMMENTARY:**

A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. You can use our screening checklist to help you decide when to do a DPIA. It is also good practice to do a DPIA for any other major project, which requires the processing of personal data.

Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.



To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

- You should consult your DPO (if you have one) and, where appropriate, individuals and relevant experts. Processors may need to assist.
- If you identify a high risk and you cannot mitigate that risk, you must consult the expert CO before starting the processing.
- The expert will give written advice within eight weeks, or 14 weeks in complex cases. In appropriate cases we may issue a formal warning not to process the data, or ban the processing altogether.

### **What's new under the GDPR?**

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk, which you cannot mitigate, you must consult the expert. This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance. Some organisations will already carry out privacy impact assessments (PIAs) as a matter of good practice. If so, you will need to review your processes to make sure they comply with GDPR requirements. The big changes are that DPIAs are now mandatory in some cases, and there are specific requirements for content and process.

If you have not already got a PIA process, you will need to design a new DPIA process and embed this into your organisational policies and procedures. In the run-up to 25<sup>th</sup> May 2018, you also need to review your existing processing operations and decide whether you need to do a DPIA for anything, which is likely to be high risk. You will not need to do a DPIA if you have already considered the relevant risks and safeguards, unless there has been a significant change to the nature, scope, context or purposes of the processing.

### **What is a DPIA?**

A DPIA is a process to systematically analyse your processing and help you identify and minimise data protection risks. It must:

- Describe the processing and your purposes;
- Assess necessity and proportionality;
- Identify and assess risks to individuals; and
- Identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified. You must do a DPIA for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability more generally and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA. It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, kept under regular review.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

### **When do you need to do a DPIA?**

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”. This means that although the actual level of risk has not been assessed yet, you need to screen for factors, which point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan to:

- Use systematic and extensive profiling with significant effects;
- Process special category or criminal offence data on a large scale; or
- Systematically monitor publicly accessible places on a large scale.

You suppose to do a DPIA if you plan to:

- Use new technologies;
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric data;
- Process genetic data;
- Match data or combine datasets from different sources;
- Collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Track individuals' location or behaviour;
- Profile children or target services at them; or
- Process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals. Even if there is no

specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

### **Art. 36 GDPR Prior Consultations**

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

- a. Where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- b. The purposes and means of the intended processing;
- c. The measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
- d. Where applicable, the contact details of the data protection officer;
- e. The data protection impact assessment provided for in Article 35; and
- f. Any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the

controller in the public interest, including processing in relation to social protection and public health.

### **Suitable Recitals**

(94) Consultation of the supervisory authority; (95) Support by the processor; (96) Consultation of the supervisory authority in the course of a legislative process.

### **COMMENTARY:**

The controller must consult the supervisory authority before the implementation of the processing only when the impact assessment conducted by the controller in application of Article 35 indicates that the processing would result in a high risk in the absence of appropriate measures taken by the controller in order to mitigate the risk (Article 36). If the authority considers that the treatment is not compliant with the Regulation, in particular if the controller has not sufficiently identified or mitigated the risk inherent to the processing, the authority then has a period of eight weeks (which may be extended by six weeks if the processing complexity so required) to advise the controller in writing - or if applicable, the processor - by exercising, if necessary, the powers referred to in Article 58 to require the provision of information, carry out investigations in the form of audit, obtain access to personal data, as well as to the premises of the controller or the processor. The final version of the Regulation specifies that the period within which the authority must give its opinion is suspended until the authority receives the information requested.

Paragraph 6 determines the terms of the request for consultation: the controller must inform the supervisory authority on the allocation of responsibilities between the controller, the possible joint controllers and the processors; the purposes and the methods of processing; measures and safeguards provided to protect the rights and freedoms of data subjects; if necessary, contact details of the data protection officer; the impact analysis carried out and any other information requested by the supervisory authority.

As this already existed in some countries, the Regulation provides that Member States shall consult the supervisory authority as part of the preparation of a proposal for a legislative measure or a regulatory measure relating to personal data processing (paragraph 4). Member States may also require that the controllers consult the supervisory authority and have its prior approval for the processing of data carried out in the context of a task performed in the public interest, including the processing of data relating to social protection and public health.

Article 20 of the Directive required Member States to define categories of processing called "at risk" i.e., those likely to present specific risks to the rights and freedoms of the data subjects. These included categories of processing that, because of their nature, scope or purposes are likely to exclude individuals from benefiting from a right, provision or contract, or those who may present risks, due to the particular use of a new technology (see recital 53). Before these categories of processing are carried out, prior evaluations were to be made by the supervisory authority or the data protection officer in cooperation with the supervisory authority.

Such prior evaluation could also be made in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

## **Section 4: Data Protection Officer**

### **Art. 37 GDPR Designation of the data protection officer**

1. The controller and the processor shall designate a data protection officer in any case where:
  - a. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
  - b. The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
  - c. The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39.
6. The data protection officer may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

### **Suitable Recitals**

(97) Data protection officer.

**COMMENTARY:**

Under Article 37 of the General Data Protection Regulation (GDPR), all public authorities and bodies will be required to designate a Data Protection Officer (DPO). Private sector organisations that on a large scale as part of their core activities regularly and systematically monitor data subjects or process sensitive personal data will also have to appoint a DPO.

On December 16, the Article 29 Working Party (WP29) published its draft guidelines on the role of the DPO, clarifying its interpretation of the GDPR as it relates to the role of the DPO. One of the most significant changes in the GDPR is the requirement for controllers and processors to be able to demonstrate compliance with the Regulation. As the WP29 puts it, the DPO is “a cornerstone” of this principle of “accountability”. That said, the WP29 emphasises that compliance is the controller’s or processor’s responsibility and DPOs are not personally responsible for compliance with the GDPR.

The terms “public authority or body”, “core activities”, “large scale” and “regular and systematic monitoring” aren’t defined in the GDPR, so the WP29 offers its interpretation and guidance on their meaning. The WP29 considers that such a notion “public authority or body” is to be determined under national law. Accordingly, public authorities and bodies include national, regional and local authorities, but the concept, under the applicable national laws, typically also includes a range of other bodies governed by public law.

‘Core activities’ can be considered as the key operations to achieve the controller’s or processor’s objectives. Regular and systematic monitoring of data subjects clearly includes all forms of tracking and profiling on the Internet, including for the purposes of behavioural advertising. However, the notion of monitoring is not restricted to the online environment. Factors to be considered when deciding whether processing is “large scale” include the number of data subjects, the volume & range of data, duration of data processing and geographical extent of data processing. A simple example given is the processing of healthcare related data by an individual doctor (not large scale), or by a hospital (large scale).

The WP29 goes on to recommend that, unless a DPO is obviously not required, controllers and processors should document the analysis and process leading to their decisions whether or not to appoint a DPO. DPOs may be appointed on a voluntary basis, but where they are, the same GDPR requirements regarding their designation, role and tasks will apply as to mandatory DPO appointments. Therefore, where organisations don’t appoint a DPO but do, as they may, assign data protection related tasks to their staff or external consultants, it should be made clear internally and externally that such staff or consultants are not DPOs.

The GDPR provides that DPOs “shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks set out in the Regulation”. There is no particular

qualification or certification specified in the Regulation, but the WP29 considers the necessary skills and expertise to include:

- Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- Understanding of the processing operations carried out;
- Understanding of information technologies and data security; knowledge of the business sector and the organisation;
- Ability to promote a data protection culture within the organisation.

The role of the DPO may be contracted out to an external service provider and, where it is, the DPO may be a natural person or a legal person (e.g., a limited company). In the latter case, the WP29 recommends that for reasons of legal clarity and good organisation, the contractor should designate a named person as the lead contact for the client.

The DPO does not necessarily have to be a full time role, but as the WP29 put it, “the DPO’s primary concern should be enabling compliance with the GDPR” and “having sufficient time to devote to DPO tasks is paramount”. Where DPOs have other duties, these cannot be incompatible with their DPO functions. Examples given by the WP29 of roles, which would conflict with the DPO's duties include:

- Chief Executive Officer;
- Chief Operating Officer;
- Chief Financial Officer;
- Chief Medical Officer;
- Head of Marketing;
- Head of Human Resources;
- Head of IT.

### **Art. 38 GDPR Position of the data protection officer**

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues, which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his

tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfill other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

### **Suitable Recitals**

(97) Data protection officer.

### **COMMENTARY:**

Article 38 imposes on the controller or the processor a series of obligations to allow the latter to undertake the tasks provided for in Article 39. So, the controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues, which relate to the protection of personal data. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

It is the responsibility of the controller or the processor to ensure the independence of the data protection officer in the performance of his or her tasks. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law (Article 38 (5)). The final version of the Regulation states further that data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights (see Article 38 (4)). Finally, the data protection officer may fulfill other tasks and duties, the controller and the processor being required to ensure that any such tasks and duties do not result in a conflict of interests.

The Directive did not say much as to the functions of the data protection officer: according to article 18, his or her task was to ensure that processing operations do not affect the rights and freedoms of the data subjects, by ensuring, in an independent way, the compliance of the processing with the national provisions



transposing the Directive. In particular, the data protection officer had to maintain records of the processing carried out by the controller, that had to contain information that were subject to notification to the competent national supervisory authority, in accordance with article 21 (2) of the Directive.

### **Art. 39 GDPR Tasks of the data protection officer**

1. The data protection officer shall have at least the following tasks:
  - a. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
  - b. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
  - c. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
  - d. To cooperate with the supervisory authority;
  - e. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

### **Suitable Recitals**

(97) Data protection officer.

### **COMMENTARY:**

#### **Data Protection Officer**

The Data Protection Officer (DPO) role is an important GDPR innovation and a cornerstone of the GDPR's accountability-based compliance framework. In addition to supporting an organisation's compliance with the GDPR, DPOs will have an essential role in acting as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation). The DPO will have professional standing, independence, expert knowledge of data protection and, to quote the GDPR, be 'involved properly and in a timely manner' in all issues relating to the protection of personal data.

The DPC recommends that all organisations who will be required by the GDPR to appoint a DPO should do this as soon as possible and well in advance of May 2018. With the authority to carry out their critical function, the Data Protection Officer will

be of pivotal importance to an organisation's preparations for the GDPR and meeting the accountability obligations.

A DPO may be a member of staff at the appropriate level with the appropriate training, an external DPO, or one shared by a group of organisations, which are all options provided for in the GDPR.

It is important to note that DPOs are not personally responsible where an organisation does not comply with the GDPR. The GDPR makes it clear that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is in accordance with the GDPR. Data protection compliance is ultimately the responsibility of the controller or the processor.

### **Who needs a DPO?**

1. All public authorities and bodies, including government departments.
2. Where the core activities of the organisation (controller or processor) consist of data processing operations, which require regular and systematic monitoring of individuals on a large scale.
3. Where the core activities of the organisation consist of special categories of data (i.e. health data) or personal data relating to criminal convictions or offences.

### **Public Authority or Body?**

Public authorities and bodies include national, regional and local authorities, but the concept typically also includes a range of other bodies governed by public law. It is recommended, as a good practice, that private organisations carrying out public tasks or exercising public authority should designate a DPO. Core activities can be defined as the key operations necessary to achieve an organisation's (controller or processor's) goals. For example, a private security company which carries out surveillance of private shopping centres and/or public spaces using CCTV would be required to appoint a DPO as surveillance is a core activity of the company. On the other hand, it would not be mandatory to appoint a DPO where an organisation undertakes activities such as payroll and IT support as, while these involve the processing of personal data, they are considered ancillary rather than core activities.

### **Large-scale processing**

While the GDPR does not define large-scale the following factors should be taken into consideration;

- The number of individuals (data subjects) concerned – either as a specific number or as a proportion of the relevant population
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

**Examples of large-scale processing include:**

- Processing of patient data in the regular course of business by a hospital
- Processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- Processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services
- Processing of customer data in the regular course of business by an insurance company or a bank
- Processing of personal data for behavioural advertising by a search engine
- Processing of data (content, traffic, location) by telephone or internet service providers

**Examples that do not constitute large-scale processing include:**

- Processing of patient data by an individual doctor
- Processing of personal data relating to criminal convictions and offences by an individual lawyer

**Regular and systematic monitoring**

Regular and systematic monitoring should be interpreted, in particular, as including all forms of tracking and profiling on the Internet, including for behavioural advertising. However, the definition of monitoring is not restricted to the online environment. Online tracking is just one example of monitoring the behaviour of individuals.

**'Regular'** is interpreted by the Working Party 29 (comprising the EU's data protection authorities) as meaning one or more of the following:

- Ongoing or occurring at particular intervals for a particular period
- Recurring or repeated at fixed times

**'Systematic'** is interpreted as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

Examples would likely include operating a telecommunications network; data driven marketing activities; profiling and scoring for purposes of risk assessment (eg fraud, credit scoring, insurance premiums); loyalty programmes, CCTV, and connected devices (eg smart cars)

## **Special Categories of Data**

These include personal data revealing; racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions and offences.

## **Further information and guidance**

Further information and guidance on the Data Protection Officer role is set out in the guidelines of the Working Party 29. In particular, these guidelines set out the position of the EU's data protection authorities on matters such as:

- Designation of a single DPO for several organisations
- Expertise and skills of the DPO
- Role, tasks, responsibilities and independence of the DPO
- Resources that should be provided to a DPO to carry out their tasks

## **Qualifications**

Article 37.5 of the GDPR provides that a Data Protection Officer "shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39." The GDPR does not define the professional qualities required or prescribe the training a DPO should undergo to be qualified to undertake the role. This allows organisations to decide on their DPO's qualifications and training tailored to the context of the organisation's data processing.

The appropriate level of qualification and expert knowledge should be determined according to the personal data processing operations carried out, the complexity and scale of data processing, the sensitivity of the data processed and the protection required for the data being processed.

For example, where a data processing activity is particularly complex, or where a large volume or sensitive data is involved (i.e. an internet or insurance company), the DPO may need a higher level of expertise and support.

Relevant skills and expertise include: expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR; understanding of the processing operations carried out; understanding of information technologies and data security; knowledge of the business sector and the organisation; and ability to promote a data protection culture within the organisation. For example, a DPO may need an expert level of knowledge in certain specific IT functions, international data transfers, or familiarity with sector-specific data protection practices such as public sector data processing and data sharing, to adequately perform their duties.

Taking into account the scale, complexity and sensitivity of their data processing operations, organisations should proactively decide on the qualifications and level of training required for their Data Protection Officer. In undertaking such an assessment, organisations should be aware that there are various training options that may be pursued. Some training courses are one-day sessions, while some are online only. Others lead to academically accredited certificates such as diplomas from national law societies. There are also other professional training programmes, which are recognised internationally, and that offer professional qualifications that require an ongoing commitment to training in order to maintain the professional qualification. The Data Protection Commissioner recommends that the following non-exhaustive list of factors be taken into consideration when selecting the appropriate DPO training programme:

- The content and means of the training and assessment;
- Whether training leading to certification is required;
- The standing of the accrediting body; and
- Whether the training and certification is recognised internationally.

In any case, a Data Protection Officer should have an appropriate level of expertise in data protection law and practices to enable them to carry out their critical role.

### **Conflict of Interests**

It is important to take into account that while a DPO is permitted to fulfill other tasks and duties, the organisation is required to ensure that any such tasks and duties do not result in a conflict of interests. This is essential to protecting the independence of the DPO. In particular, it means that a DPO cannot hold a position in an organisation where they have the authority to decide the purposes for which personal data is processed and the means by which it is processed. While each organisational structure should be considered case by case, as a rule of thumb, conflicting positions within an organisation may include senior management positions such as chief executive, chief operating/financial/medical officer, head of HR or head of IT. The WP29 guidelines address this matter in further detail.

### **Publication and communication of the DPO's contact details**

Organisations will be required by the GDPR to publish contact details of the DPO and to communicate these details to the relevant data protection authority. The purpose of this requirement is to ensure that individuals (internal and external to the organisation) and the data protection authority can easily and directly contact the DPO without having to contact another part of the organisation.

## Section 5: Codes of conduct and certification

### Art. 40 GDPR Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

- a. Fair and transparent processing;
- b. The legitimate interests pursued by controllers in specific contexts;
- c. The collection of personal data;
- d. The Pseudonymisation of personal data;
- e. The information provided to the public and to data subjects;
- f. The exercise of the rights of data subjects;
- g. The information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- h. The measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
- i. The notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
- j. The transfer of personal data to third countries or international organisations; or
- k. Out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority, which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes, which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

### **Suitable Recitals**

(98) Preparation of codes of conduct by organisations and associations; (99) Consultation of stakeholders and data subjects in the development of codes of conduct.

**COMMENTARY:**

- The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.
- The specific needs of micro, small and medium sized enterprises must be taken into account.
- Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.
- Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:
  - improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
  - provide mitigation against enforcement action; and
  - improve standards by establishing best practice.
- When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

**Who is responsible for drawing up codes of conduct?**

- Governments and regulators can encourage the drawing up of codes of conduct.
- Codes of conduct may be created by trade associations or representative bodies.
- Codes should be prepared in consultation with relevant stakeholders, including individuals (Recital 99).
- Codes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB).
- Existing codes can be amended or extended to comply with the requirements under the GDPR.

**What will codes of conduct address?**

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the Pseudonymisation of personal data;



- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

### **What are the practical implications?**

If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority. If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover. Adherence to a code of conduct may serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.

### **Who is responsible for certification mechanisms?**

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation. Certification will be issued by supervisory authorities or accredited certification bodies.

### **What is the purpose of a certification mechanism?**

A certification mechanism is a way of you demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures. A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers. They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

### **What are the practical implications?**

Certification does not reduce your data protection responsibilities. You must provide all the necessary information and access to your processing activities to the certification body to enable it to conduct the certification procedure. Any certification will be valid for a maximum of three years. It can be withdrawn if you no longer meet the requirements of the certification, and the supervisory authority will be notified. If you fail to adhere to the standards of the certification scheme, you risk being subject to an administrative fine of up to 10 million Euros or 2 per cent of your global turnover.

Under Articles 40 and 41 of the GDPR, codes of conduct are explicitly recognized and encouraged as a way to meet security requirements. Article 32(3) (Security of

Processing) states that “adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.”

#### **Art. 41 GDPR Monitoring of approved codes of conduct**

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

- a. demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
- b. established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- c. established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- d. demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft requirements for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the requirements for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

**COMMENTARY:**

Article 41 authorises, on certain conditions, an independent body to monitor the compliance with a code of conduct approved under article 40 without prejudice to the tasks and powers of the competent supervisory authority pursuant to Articles 57 and 58. Paragraph 1 stipulates that the monitoring of compliance may be carried out only by a body, which has an appropriate level of expertise in relation to the subject-matter of the code.

The second paragraph sets out the conditions that such body must meet:

- it must have demonstrated its independence and expertise in relation to the subject-matter of the code to monitor (a);
- the body must have established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation (b);
- the body must have established transparent procedures to handle complaints about infringements of the code by a controller or processor, by guaranteeing the absence of conflicts of interest (c);
- the body must have demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests (d).

The competent supervisory authority shall submit the draft criteria as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63 (3). Without prejudice to the tasks and powers of the competent supervisory authority, such body shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them. The competent supervisory authority shall revoke the accreditation of a body if the conditions for accreditation are not met or where actions taken by the body infringe this Regulation. This provision shall not apply to processing carried out by public authorities and bodies.

There was no provision of the Directive for monitoring of the approved codes as no procedure for approval of such codes was provided. We may wonder what will be the status of the control body in national law, separate from the national supervisory authority. A priori, it will not be a public institution, but private, which would then have powers of sanctions with respect to an enterprise established as appropriate in a third country. The regulation says nothing either in terms of the management of the costs of this compulsory control, which may also pose difficulties, in addition to the management of potential conflicts of interest. Also, it should be noted that the provision does not apply to public authorities and public institutions even though they are not excluded from article 38 and are therefore required to adopt the codes.

We may also ask which conditions precisely these qualifications of public authorities meet as not defined by the Regulation.

## **Art. 42 GDPR Certification**

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the Board approves the criteria, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant criteria continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the criteria for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

### **Suitable Recitals**

(100) Certification.

### **Art. 43 GDPR Certification bodies**

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

- a. The supervisory authority which is competent pursuant to Article 55 or 56;
- b. The national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority, which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

- a. Demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
- b. Undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
- c. Established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- d. Established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- e. Demonstrated, to the satisfaction of the competent supervisory authority that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of requirements approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged

in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

## **COMMENTARY:**

### **Main elements of GDPR Articles 42 and 43**

The GDPR introduced certification as a means for a data controller or a data processor to demonstrate compliance of a processing operation with the Regulation. An additional function of certification in the context of the GDPR is to enhance transparency, since certifications, seals, and marks allow data subjects to “quickly assess the level of data protection of relevant products and services”.

### **Certification as an accountability-based mechanism**

Certification is well linked to the newly introduced principle of accountability. As already highlighted by the Article 29 Data Protection Working Party in 2010, data protection needed additional mechanisms that translate legal requirements into real data protection measures. Certification and seals are treated as accountability-based

mechanisms, due to their potential effect to facilitate scalability, compliance, transparency, and to some extent legal certainty.

Art. 5(2) GDPR requires the data controller to both comply with the principles relating to the processing of personal data and demonstrate its compliance. Demonstration of compliance in practice may require multiple actions, such as proper documentation and record keeping (in line with art. 30 GDPR). Certification can play a role in that respect; a controller that has had its processing operations successfully evaluated by a certification body may use the certification and its supporting documentation as an element to demonstrate compliance to the supervisory authority. The fact that data protection certification in the GDPR is an accountability-based mechanism is supported by its voluntary nature.

### **Certification of compliance with GDPR provisions**

As the GDPR provides in Art. 42 (4), a certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation, meaning that compliance with the GDPR is not possible to be certified. What can be certified is compliance with certification criteria that are derived from the GDPR. Compliance with such criteria entails that a controller or processor at a certain period in time has taken measures to ensure that it fulfills certain obligations, for instance to secure personal data in a given processing operation.

In general, where the EU legislature, intends to assign a different effect to certification or self-declaration of conformity, this is explicitly provided in the legislation. For instance, conformity with harmonised standards that are developed on the basis of the New Approach Directives, offer a presumption of conformity with the legislation and this is explicitly provided for in the relevant law.

### **Certification bodies and Supervisory authorities**

The data protection mechanisms as proposed in Art. 42 and 43 GDPR involve mainly the following actors:

- The data controller or data processor that aims to apply for certification ('applicant')
- The certification body
- The supervisory authority (data protection authority)
- The European Data Protection Board (EDPB)

The certification bodies and the supervisory authorities are key actors in the certification process. Certification may be conducted by either a certification body that fulfills the conditions of Art. 43 GDPR, or by a supervisory authority. The GDPR does not determine when a certification body conducts the process and when by a supervisory authority. This legal gap appears to be intentional: Member States and national supervisory authorities may organise certification at a national level according to their preferred model.

After the evaluation phase, in the case that the applicant fulfills the necessary requirements, certification is granted by the certification body or the supervisory authority. Certification is issued for three years, and may be renewed. It is important to mention that even when the certification body issues the certification, the supervisory authority has several powers, such as to withdraw the certification or order the certification body to withdraw the certification.

The supervisory authorities also have the power to approve criteria for certification. Not every certification in the field of data protection is automatically a data protection certification mechanism as provided in the GDPR. The national supervisory authority needs to formally approve the certification criteria. Such approval may constitute an administrative act, with legal effects. The European Data Protection Board (EDPB) takes the role of the national supervisory authorities, as outlined above, in the case of a European Data Protection Seal. The European Data Protection Seal is a common EU-wide certification, the criteria of which are approved not by one or more national data protection authorities, but by the European Data Protection Board.

### **Scope of certification under GDPR**

As highlighted, not every certification in the field of data protection is automatically a data protection certification mechanism as provided in the GDPR. In fact, the GDPR appears to be quite limiting when providing the scope of processing activities where data controllers and processors can use certification as an element to show compliance. The scope is mainly limited by the following conditions:

#### **1. Purpose of certification**

According to Article 42 of GDPR, “The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors”. The purpose of a data protection certification mechanism under GDPR is thus demonstrating compliance with the Regulation of processing operations by controllers and processors, which clarifies that the substantive requirements a client must fulfill must be related to the provisions of the GDPR, for example to demonstrate compliance with the provision on data security (Art. 32). If a certification mechanism involves a scope that is not in the scope of the GDPR, for example a data protection education course, such a mechanism cannot be used to demonstrate compliance with the GDPR. Such a certification mechanism would therefore not be in the scope of Art. 42 & Art. 43 of the GDPR data protection certification mechanisms. Nevertheless, such certification may exist in the free market and potentially contribute to raising the levels of data protection awareness.

#### **2. Processing operation**

The object of certification must be a processing operation. The GDPR regulates the processing of personal data, which may be conducted in the context of a product



or system or a service. However, the wording of Art. 42(1) requires that a certification mechanism under GDPR must concern an activity of data processing. Such an activity may be (also an integral) part of a product, a system, or service, but the certification must be granted in relation to the processing activities, and not to the product, system or service as such (e. g. certification of data deletion process in product X).

### **3. Controllers or processors**

The reference to “by controllers or processors” limits the scope of applicants that can opt for certification under the GDPR to controllers and processors. Producers or manufacturers of products, systems and services, if they do not process any personal data, as controllers or processors, are not in the scope of the GDPR certification mechanisms. Nevertheless, there might be certifications in the market, aimed at manufacturers (e.g. OS providers and mobile device manufacturers), in relation to data protection-friendly configuration of products or systems, which will undoubtedly contribute to raise the level of data protection. However, they will be outside of the scope of the GDPR data protection certification mechanisms of Art. 42 and 43 GDPR.

### **Accreditation of certification bodies**

A substantial part of the GDPR provisions on certification refers to accreditation. The legislature emphasizes the importance of having reliable, competent, and independent bodies carrying out the certification by devoting Art. 43 GDPR to certification bodies. Art. 43 GDPR requires the certification bodies that provide data protection certifications to be accredited. The GDPR allows the Member States to select the accreditation model they will follow, from a selection of three options:

- a. Accreditation by a Data Protection Authority (or the European Data Protection Board, in the case of the European Data Protection Seal) 27,
- b. Accreditation by the National Accreditation Body on the basis of the Accreditation Regulation and the ISO/IEC 17065:2012 standard and additional requirements in the field of data protection provided by the Data Protection Authority, or
- c. Both authorities, namely the National Accreditation Body and the competent Data Protection Authority, collaborating in this task.

\* \* \*

## **CHAPTER 5: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS**

### **Art. 44 GDPR General Principle for transfers**

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

### **Suitable Recitals**

(101) General principles for international data transfers; (102) International agreements for an appropriate level of data protection.

### **COMMENTARY:**

Article 44 is intended to state the general principle governing data transfers to non-EU third countries or international organizations. These transfers can only be effected if the controllers and the processors falling under the scope of the Regulation comply with the rules provided in Chapter V. The provision gives however a new extension to the rule: transfers of personal data to a third country or to an international organization operated as part of planned or ongoing processing are covered, but also the future processing by the recipient third country to another country or another organization. They must also comply with Chapter V of the Regulation. In other words, by this provision, the Regulation sets up a sort of data protection-specific “right to pursue”: the data transferred outside the Union remain subject to the law of the Union not only for their transfer, but also for any processing and subsequent transfer.

The concept of international organization, defined in article 4, 26) of the Regulation is an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries. This provision has been reintroduced by the final version of the Regulation, after having been removed from the second proposed version. The goal, as referred to in the provision is that the level of protection of individuals guaranteed by the Regulations is not lowered.

The extension of the territorial scope to processing carried out outside the territory of the Union, by recipient controllers and processors established outside the EU has both political and legal implications. Politically, the provision allows the European authorities to intervene and detect violations of the Regulation outside the EU on the grounds of a new legitimacy included in the Regulation. It can more easily use the argument of the data protection in different files or negotiations in order to

obtain an advantage. Legally, it goes without saying that the provision may be felt by third countries as an attack on their sovereignty because it imposes a new rule on their territory and a limitation of the freedom of processing. The powers of control and enforcement of the EU authorities and the Member States, of course, cannot be exercised outside the territory of the EU.

The measure must be taken of the difference with other rules allowing the application of the Regulation to controllers established outside the territory of the EU (see Article 3). It is an indirect submission since only the controllers and the processors who are subject to the other provisions of the Regulation pursuant to Article 3, must comply with Article 44 and accordingly, Chapter V. There is no recipient of the transferred data. Or any person concerned by the data, which would be at the origin of the transfer either.

#### **Art. 45 GDPR Transfers on the basis of an adequacy decision**

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

1. The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

2. The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

3. The international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

## Suitable Recitals

(103) Appropriate level of data protection based on an adequacy decision; (104) Criteria for an adequacy decision; (105) Consideration of international agreements for an adequacy decision; (106) Monitoring and periodic review of the level of data protection; (107) Amendment, revocation and suspension of adequacy decisions.

## COMMENTARY:

Article 45, paragraph (1) of the GDPR, The concept of “adequate level of protection” which already existed under Directive 95/46, has been further developed by the CJEU (The Court of Justice of the European Union). At this point it is important to recall the standard set by the CJEU in Schemes, namely that while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU, "the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU". Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation.

The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country or an international organization, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules.

Article 45, paragraph (2) of the GDPR, establishes the elements that the European Commission shall take into account when assessing the adequacy of the level of protection in a third country or international organization. For example, the Commission shall take into consideration the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organization has entered into.

It is therefore clear that any meaningful analysis of adequate protection must comprise the two basic elements: the content of the rules applicable and the means for ensuring their effective application. It is upon the European Commission to verify – on a regular basis - that the rules in place are effective in practice. The ‘core’ of data protection ‘content’ principles and ‘procedural/enforcement’ requirements, which could be seen as a minimum requirement for protection to be adequate, are derived from the EU Charter of Fundamental Rights and the GDPR. In addition,

consideration should also be given to other international agreements on data protection, e.g. Convention 108. Attention must also be paid to the legal framework for the access of public authorities to personal data.

General provisions regarding data protection and privacy in the third country are not sufficient. On the contrary, specific provisions addressing concrete needs for practically relevant aspects of the right to data protection must be included in the third country's or international organization's legal framework. These provisions have to be enforceable. According to Article 45 (4) of the GDPR it is upon the European Commission to monitor – on an ongoing basis - developments that could affect the functioning of an adequacy decision.

Article 45 (3) of the GDPR provides that a periodic review must take place at least every four years. This is, however, a general time frame which must be adjusted to each third country or international organization with an adequacy decision. Depending on the particular circumstances at hand, a shorter review cycle could be warranted. Also, incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule. It also appears to be appropriate to have a first review of an entirely new adequacy decision rather soon and gradually adjust the review cycle depending on the outcome.

Given the mandate to provide the European Commission with an opinion on whether the third country, a territory or one or more specified sectors in this third country or an international organization, no longer ensures an adequate level of protection, the EDPB must, in due time, receive meaningful information regarding the monitoring of the relevant developments in that third country or international organization by the EU Commission. Hence, the EDPB should be kept informed of any review process and review mission in the third country or to the international organization. The EDPB would appreciate to be invited to participate in these review processes and missions.

It should also be noted that according to Article 45 (5) of the GDPR the European Commission has the right to repeal, amend or suspend existing adequacy decisions. The procedure to repeal, amend or suspend should consequently involve the EDPB by requesting its opinion pursuant Art. 70(1) (s).

#### **Art. 46 GDPR Transfers subject to appropriate safeguards**

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

1. A legally binding and enforceable instrument between public authorities or bodies;
  2. Binding corporate rules in accordance with Article 47;
  3. Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
  4. Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
  5. An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
  6. An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
1. Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
  2. Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
  4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.
  5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

### **Suitable Recitals**

(108) Appropriate safeguards; (109) Standard data protection clauses.

### **COMMENTARY:**

#### **Transfers on the Basis of “Appropriate Safeguards”**

When the Directive was passed in 1995, it anticipated that many countries would not have the benefit of an adequacy decision. For such situations, it introduced the possibility of basing data transfers to non-EU countries on what came to be termed “appropriate safeguards” for individuals. “Appropriate safeguards”

referred to legally binding commitments by companies to provide adequate protection over individuals' data, backed up by effective legal remedies for both affected individuals and European DPAs.

In data protection literature, these transfer mechanisms are often referred to as “alternative transfer tools” or “alternative transfer mechanisms”—an allusion to the fact that while a Commission adequacy decision may represent the ideal basis for international data transfers, “appropriate safeguards” remain as alternatives for companies in countries where no adequacy decision exists.

“Appropriate safeguard” mechanisms developed under the Directive for permitting transatlantic data transfers include model contractual clauses (“model clauses”) and binding corporate rules (BCRs). The GDPR expressly recognizes and permits both of these mechanisms. Additionally, the GDPR creates new transfer mechanisms in the form of approved codes of conduct and certifications. In the following, we will briefly sketch each alternative transfer mechanism, as well as address some of the practical considerations associated with implementing them under the GDPR.

## **1. Model Clauses**

Model clauses have proven particularly useful for companies that engage in large and routine transfers of data from the EU to the U.S. Many large and recognizable U.S. companies use model clauses as the basis of data flows from customers and subsidiaries because they are standardized and (by law) nonnegotiable, which make them advantageous for standard terms as well as for intra corporate arm's-length agreements.

### **a. Model Clauses under the GDPR**

Like the Directive, the GDPR continues to permit transfers on the basis of model clauses. To use the GDPR's language, “standard data protection clauses adopted by the Commission” constitute “appropriate safeguards” that permit data transfers to non-EU countries even in the absence of an adequacy decision. Moreover, the GDPR expressly provides that model clauses adopted under the Directive will continue in force under the GDPR until amended, replaced, or repealed. Practically speaking, this means that companies that have model clauses in place that predate the GDPR will be able to continue relying on them after the GDPR enters into force in May 2018.

Additionally, the GDPR expands the possibilities for model clauses in the future. In addition to the Commission's already-existing model clauses, the GDPR now grants national DPAs the authority to adopt their own “standard data protection clauses.” To do so, DPAs must first present proposed model clauses to the Commission for approval. If the Commission approves, companies subject to that DPA's jurisdiction can take advantage of its model clauses as a basis for international data transfers. This ground may be useful for the development of model clauses that accommodate specific sectorial needs, such as the cloud or travel sector.



On a helpful note, the GDPR codifies several practices that developed under the Directive among certain DPAs regarding model clauses. This ensures these practices will be available EU-wide and not merely in isolated jurisdictions:

To date, the Commission has adopted only controller-to-controller and controller-to-processor model clauses—but no model clauses for processor-to-processor (P2P) transfers. Although model P2P clauses have long been discussed in the EU, and the Article 29 Working Party even went so far as to draft (but not finalize) such clauses, model P2P clauses are presently a rarity in the EU. The GDPR permits both the Commission as well as national DPAs to adopt model P2P clauses.

Finally, the GDPR allows companies to draft ad hoc data transfer agreements and submit them to the competent DPA for approval. These can also be processor-to-processor clauses. It is expected that most DPAs will require ad hoc agreements to largely reflect the provisions of the model clauses (even if that is not a formal requirement).

#### **Art. 47 GDPR Binding corporate rules**

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

- a. Are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- b. Expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- c. fulfill the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

- a. The structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- b. The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- c. Their legally binding nature, both internally and externally;
- d. The application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- e. The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on

automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

f. The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

g. How the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

h. The tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

i. The complaint procedures;

j. The mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

k. The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

l. The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

m. The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

n. The appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

### **Suitable Recitals**

(110) Binding corporate rules.

### **COMMENTARY:**

It should be recalled that BCR-P (BCRs for processors) apply to data received from a controller established in the EU which is not a member of the group and then processed by the group members as processors and/or sub processors; whereas BCRs for Controllers (BCR-C) are suitable for framing transfers of personal data from controllers established in the EU to other controllers or to processors established outside the EU within the same group. Hence the obligations set out in the BCR-P apply in relation to third party personal data that are processed by a member of the group as a processor according to the instructions from a non-group controller.

Taking into account that Article 47.2 of the GDPR lists a minimum set of elements to be contained within a BCR, this amended table is meant to: - Adjust the wording of the previous referential so as to bring it in line with Article 47 GDPR, - Clarify the necessary content of a BCR as stated in Article 47 and in document WP 2041 adopted by the WP29 within the framework of the Directive 95/46/EC, - Make the distinction between what must be included in BCRs and what must be presented to the competent Supervisory Authority in the BCRs application (document WP 195a2), and - Provide explanations/comments on each of the requirements. Article 47 of the GDPR is clearly modeled on the Working documents relating to BCRs adopted by the WP29. However, it specifies some new elements that need to be taken into account when updating already existing approved BCRs or adopting new sets of BCRs so as to ensure their compatibility with the new framework established by the GDPR.

Binding Corporate Rules (BCRs) are an intra company code of conduct that regulates the principles and rules that apply to the processing and transfer of personal data within a company group, including cross-border. BCRs were established through the standard practice of data protection authorities (DPAs) and the guidance of the Article 29 Working Party (WP29). The upcoming General Data Protection Regulation (GDPR) explicitly recognizes BCRs, both for controllers (BCR-C) and processors (BCR-P). It also extends the scope of application not only to a corporate group but also to a group of enterprises engaged in a joint economic activity, for instance joint ventures.

After WP29 endorsed BCR-C as a useful mechanism for data transfers of complex international structures in 2003, several companies adopted them. Instead of having to justify international transfers on an individual basis, and concluding model contracts with numerous parties, BCRs allow a single set of transfer rules for

the entire company group. In today's interconnected world, it is increasingly important to easily transfer data wherever needed, and BCRs offer the flexibility required for such elaborate transfers.

A framework for BCR-Ps was introduced much later, in 2012, and their further inclusion in the GDPR was fiercely debated. In endorsing their inclusion, WP29 praised the merits of BCR-P as an optimal solution for international data transfers. At the same time, WP29 held that BCR-P provides more transparency and accountability requirements beyond those provided in model clauses or other transfer mechanisms (e.g., the current Privacy Shield).

### **Increased Flexibility**

BCRs will become more flexible under the GDPR. Under the current regime, countries have to first approve their BCRs in all relevant countries through mutual recognition or a cooperation procedure. They still need to obtain national DPA authorizations in certain countries to allow for the transfer of personal data under the BCRs. These transfer permits only allow specific transfers, and any time a company wants to expand or alter its transfers, a new notification and permitting procedure is required. Making things more complicated, BCRs are not recognized in Portugal as a valid legal basis to transfer personal data outside of the European Economic Area (EEA).

The GDPR does not contain DPA notification and authorization requirements for data transfers. National authorizations of BCRs will be abolished, which will significantly reduce the time required to introduce a BCR and will increase flexibility altogether. Because of the direct applicability of the GDPR in all EU member states, any remaining inconsistencies (e.g., Portugal) will be automatically ironed out. As a result, processors will likely increasingly rely on BCR-Ps to justify transfers outside the EEA since they will be able to engage in practically unlimited data transfers within their company groups.

### **Demonstrate Accountability**

Under the GDPR, the data transfer rules are also directly applicable to processors. Processors should, therefore, no longer be dependent on data transfer mechanisms put in place by controllers, but rather have their own tools available to comply with these requirements. Besides, WP29 has indicated that a BCR is an organizational accountability tool that has many merits beyond contractual solutions such as the EC model clauses. For intragroup transfers, BCR-P not only provides a good basis for transfers but also helps demonstrate broader compliance with the GDPR, for instance the principles of accountability, lawfulness of processing, general processing requirements, and security of processing.

### **Meet the By-Default and By-Design Requirement and Avoid High Fines**

GDPR refers to the requirement of ensuring data protection by design and by default. Therefore, companies should introduce appropriate technical and organizational measures so that all the data protection principles are met. This is a

relatively wide concept, and high GDPR fines (up to 4% of a company's global turnover or €20 million, whichever is higher) leave no room for experimentation.

To this end, the GDPR provides that an approved certification mechanism, like a BCR-P, may be used as an element to demonstrate compliance with the by-design and by-default requirements. This tangible uplift in compliance may save companies substantial amounts of money.

### **Reduce a Company's Operational Cost and Administrative Burden**

A BCR-P can also reduce a company's overall operational cost. While a processor, a company may be required to make several cross-border transfers across the globe. If it opts for Model Clauses, for example, the overall cost of the process will be higher, and the administrative burden of dealing with several different schemes particularly heavy. The cost of a BCR is significant in the beginning, yet once in place, less time and money is required for daily company operations.

### **Enhance Customer Confidence**

A BCR is a very detailed code of conduct that exposes a company's policies and procedures to regulators and the public. Once enforced, a BCR signals to customers that the company takes its data protection duties very seriously and that their data is in safe hands. Processors may operate in various sensitive industries (e.g., financial services, telecoms, technology) where reputation is extremely important and may have a significant impact on a company's viability and profitability. BCRs communicate a transparent, robust, and holistic data protection approach.

### **Future Procedural Flexibility**

The GDPR gives leeway to the European Commission, upon consultation with the newly introduced European Data Protection Board (EDPB), to create procedural rules in the future to better facilitate the approval process. Since the European Commission may specify the format and procedures for BCR-Ps, it is likely we will experience model BCR approval procedures, which may streamline the BCR approval process even further.

## **Art. 48 GDPR Transfers or disclosures not authorised by Union law**

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

### **Suitable Recitals**

(115) Rules in third countries contrary to the Regulation.

**COMMENTARY:**

There is no analogous provision under the Directive. To understand whether or not Art. 48 will complicate discovery requires not only understanding how the EU will interpret and apply this provision and its requirements, but also how courts in the other country will interpret the Article. As explained, the legislative bodies have ultimately decided to include Art. 48 in order to specifically regulate requests from a court, tribunal, or administrative authority, which is based in a third country (i.e., a country outside of the European Economic Area).

Since such provision cannot be found in the Directive 95/46/EC, as the current data protection regime in the EU which national laws are based on, it is questionable how the new Art. 48 will be interpreted and if and how it will ultimately change the legal requirements when it comes to dealing with discovery requests from third countries.

**Art. 49 GDPR Derogations for specific situations**

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- a. The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- b. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- c. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- d. The transfer is necessary for important reasons of public interest;
- e. The transfer is necessary for the establishment, exercise or defence of legal claims;
- f. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- g. The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

### **Suitable Recitals**

(111) Exceptions for certain cases of international transfers; (112) Data transfers due to important reasons of public interest; (113) Transfers qualified as not repetitive and that only concern a limited number of data subjects; (114) Safeguarding of enforceability of rights and obligations in the absence of an adequacy decision; (115) Rules in third countries contrary to the Regulation.

### **COMMENTARY:**

The derogations provided for by the Directive have been maintained and developed in Article 49 of the Regulation. Subject to several adaptations, the derogations already covered by Directive are set out here, such as:

- The explicit consent of the data subject for the transfer (a). Since this derogation is based on consent, the commented provision requires the controller to obtain the “explicit” consent of the data subject to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- When the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request (b);
- When the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (c);
- When the transfer is necessary for important reasons of public interest (d). Recital 112 provides several examples of data transfer needed for important reasons of general interest: in case of international exchange of data between competition authorities, tax or customs administrations, between financial supervisory authorities, between services responsible for matters of social security or public health. In this regard, article 49 (4) specifies that the general interest justifying the transfer must be recognized by the EU law or the national law of the Member State of the controller;
- when the transfer is necessary for the establishment, exercise or defence of legal claims (e);
- When the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent (f). The derogation relating to the vital interests of the data subject, now also seeks the protection of vital interest of others.
- When the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest. The consultation conditions must be met in compliance with the Union or Member State law (g). Paragraph 2 restricts the data that can be subject of a transfer in this case. Such transfer shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Finally, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

The essential innovation of Article 49 is the introduction of a new derogation based on the need for the transfer for the purpose of compelling legitimate interests pursued by the controller or the processor; resorting to this derogation is however strictly controlled.

To invoke this derogation, the transfer



- Cannot be based on Articles 45 (adequate level of protection) or 46 (sufficient safeguards) including those related to the binding corporate rules (Article 47) or any other derogations referred to in Articles 49 (1), (a) to (f);
- Must not be repetitive, concerns only a limited number of data subjects, which means to take into consideration the amount of personal data and the number of data subjects and to consider whether the transfer is carried out on an occasional or regular basis.
- Must be necessary in the pursuit of “incontestable” legitimate interests of the controller which are not overridden by the interests or rights and freedoms of the data subject;
- The controller or the processor has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. This means that the controller should take into consideration the nature of the data, the purpose and duration of envisaged processing as well as the situation in the country of origin, in the third country and the country of final destination and provide appropriate safeguards to protect fundamental rights and freedoms of natural persons. The final version of the regulation adds that the controller or the processor must document the above assessment and the safeguards taken accordingly (6).
- The controller must not only notify the supervisory authority of said transfer but must also provide additional information to the data subjects regarding the compelling interests that justify the transfer of their data, in addition to the information referred to in articles 13 and 14.

It should be noted that the derogations based on the consent of the data subject, on the contractual need (that is, the exceptions referred to in articles 49 (1) (b) and (c), as well as on compelling legitimate interests of the controller, are not applicable to the activities of the public authorities in the exercise of their prerogative of public power (paragraph 3).

Finally, according to paragraph 5, in the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organization.

Article 26 of the Directive formulated six exceptions to the prohibition to transfer data to a third country not providing an adequate level of protection. They addressed limited cases presenting risks normally mitigated for the data subject, taking account of the primacy of the public interest or that of the data subject over data protection. According to the Article 29 Working Party, resorting to these exemptions should be the ultimate solution only, when no other provision was made to allow the transfer (G29, Working Document of 24 July 1998, Transfers of Personal Data to Third Countries: Application of Articles 25 and 26 of the Directive on the Data Protection, WP 12).

These exemptions addressed the following cases: when the data subject had given his explicit consent to the transfer; when the transfer was necessary in the context of a contract or a legal action; when the protection of an important public interest demanded it; or for recognition, exercise or defence of a legal right, for example in the case of international exchange of data between tax or customs administrations or between services competent for social security; when the transfer was necessary to protect the vital interest of the data subject, or when the transfer was made from a register established by law and intended to be viewed by the public or by persons who can prove a legitimate interest.

These exceptions were subject to a strict interpretation, as advocated by the Article 29 Working Party in its Working Paper No. 114 on a common interpretation of the provisions of Article 26 (1) of Directive 95/46/EC of 24 October 1995 adopted on 25 November 2005, as after their transfer, these have no protection.

Article 49 contains the traditional exceptions, already implemented by the Directive. The provision, in admitting an exception to the prohibition of transfer on the basis of indisputable legitimate interests of the controller, is also aimed to facilitate the admission of exceptional transfers to third countries without an adequate level of protection, while safeguarding the rights of the data subject. It could be particularly useful in the event that the data is transferred to a processor outside the EU.

### **Art. 50 GDPR International cooperation for the protection of personal data**

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

1. Develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
2. Provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
3. Engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
4. Promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

### **Suitable Recitals**

(116) Cooperation among supervisory authorities.

### **COMMENTARY:**

In relation to third countries and international organizations, Article 50 requires the Commission and the supervisory authorities to take certain measures in order to facilitate the application of the data protection principles. This provision takes into account the recommendation of the Organization for Economic Cooperation and Development (OECD) of 12<sup>th</sup> June 2007 on the cross-border cooperation in the application of the laws protecting privacy.

These measures are intended to develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data (paragraph 1 (a)); They should then provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms (paragraph 1 (b));

These mechanisms are intended, on the one hand, to engage the relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data (paragraph 1 (c)); and, on the other hand, to promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries (paragraph 1 (d)).

The Directive did not envisage the possibility of cooperation between the Member States and non-Union third countries or international organizations.

\* \* \*

## CHAPTER 6: INDEPENDENT SUPERVISORY AUTHORITIES

### Section 1: Independent status

#### Art. 51 GDPR Supervisory Authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority, which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.
4. Each Member State shall notify to the Commission the provisions of its law, which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

#### Suitable Recitals

(117) Establishment of supervisory authorities; (118) Monitoring of the supervisory authorities; (119) Organisation of several supervisory authorities of a Member State; (120) Features of supervisory authorities.

#### COMMENTARY:

The GDPR

As provided for in the Directive, Article 51 requires the Member States to set up one or several independent supervisory authorities responsible for the monitoring of the application of the Regulation.

The supervisory authority is defined in article 4 (21), as "an independent public authority, which is established by a Member State pursuant to Article 51". The final version of the Regulation specifies that these authorities are intended, on the one hand, to protect the fundamental rights and freedoms of natural persons in relation to processing, and on the other, facilitate the free flow of personal data within the Union.

According to paragraph 2, each supervisory authority shall contribute to the consistent application of the Regulations throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

It should be noted that the Regulation expressly allows the Member States to create several control authorities. In this case, the Member State shall designate the supervisory authority, which is to represent those authorities on the European Data Protection Board. The Member State shall also set out the mechanism to ensure compliance by other authorities with the rules relating to the consistency mechanism referred to in Article 63.

All the provisions adopted by a Member State under Chapter VI must be notified to the Commission no later than two years after the entry into force of the Regulation, that is, the 20th day following its publication in the Official Journal of the European Union (Art. 99). Any subsequent changes must be notified to the Commission without delay.

The Directive contained an essential element of data protection: the establishment in each Member State of a supervisory authority responsible for monitoring the application of the personal data protection legislation on its territory. The second paragraph of Article 28 of the Directive already stated that the tasks entrusted to these authorities should be carried out independently. The Member States have each created a national supervisory authority for the protection of personal data.

## **Art. 52 GDPR Independence**

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff, which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

## Suitable Recitals

(117) Establishment of supervisory authorities; (118) Monitoring of the supervisory authorities; (120) Features of supervisory authorities; (121) Independence of the supervisory authorities.

## COMMENTARY:

Article 52 is intended to clarify the conditions guaranteeing the independence of the supervisory authorities, in accordance with the case law of the Court of Justice of the European Union (CJEU, 9 March 2010, C-518/07), and also on the basis of Article 44 of Regulation (EC) No. 45/200135.

In this case, the Court considered that the Federal Republic of Germany had failed to fulfill the obligations imposed under Article 28, paragraph 1, second subparagraph of Directive 95/46 by submitting to the guardianship of the State the supervisory authorities competent for monitoring the personal data processing by the non-public sector in the different countries, thus transposing incorrectly the requirement that these authorities exercise their tasks “with complete independence”.

Furthermore, Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data provides in details the conditions of independence of the European data protection controller.

Article 52 codifies that the supervisory authority of each Member State shall act with complete independence in performing its tasks and exercising its powers, in accordance with this Regulation. Accordingly, the second paragraph of Article 52 specifies that member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

The third paragraph obliges the members of the supervisory authority to refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether profitable or not (Art. 52 (3)). Pursuant to paragraph 4, each Member State shall ensure that each supervisory authority is provided with the staff, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the European Data Protection Board.

Each supervisory authority must also be able to choose and have its own staff, which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

Finally, as stated in recital 118, the independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial management. Accordingly, Article 52, paragraph 6 provides that each supervisory authority is subject to financial control, which does not affect its independence. For this purpose, each supervisory authority shall have a separate, public annual budget, which may be part of the overall state or national budget. According to Article 28, paragraph 1, second subparagraph of the Directive, the national authorities shall act with complete independence in exercising the functions entrusted to them.

### **Art. 53 GDPR General conditions for the members of the supervisory authority**

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

- their parliament;
- their government;
- their head of State;
- an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfills the conditions required for the performance of the duties.

### **Suitable Recitals**

(121) Independence of the supervisory authorities.

### **COMMENTARY:**

The GDPR

Article 53 sets out the general conditions of the status applicable to the members of the supervisory authority, in accordance with the case law of the CJEU (see CJEU, 9 March 2010, C-518/07), and on the basis also of article 42, paragraphs 2 to 6 of the Regulation (EC) No. 45/2001 on the processing of data carried out by the institutions and bodies of the European Union.

Initially, recital 121 recommended that the conditions applicable to the members are determined by the law of each Member State and that the appointment of members is made by the parliament or by the federal government. The second proposed version of the Regulation has somewhat eased the principles established by the above-mentioned recital by providing that members of the supervisory

authority may also be appointed by an independent body. Thus, Article 53 in its first paragraph provides that the members of the supervisory authorities be appointed by means of a transparent procedure by either their parliament or government, by the head of their state or by an independent body entrusted with the appointment under Member State law (Art. 53 (1)).

According to the second paragraph, each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

Article 53 provides several guarantees of independence in favour of members of the national authority: first the duties of a member shall end in the event of the expiry of the term of office, or resignation or compulsory retirement in accordance with the law of the Member State concerned. The final version of the Regulation adds that a member shall be dismissed only in cases of serious misconduct or if the member no longer fulfills the conditions required for the performance of the duties.

#### The Directive

The Directive does not say much about the status of the members of the supervisory authority. At most, Article 28 (7) of the Directive imposed to the Member States the obligation to provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

### **Art. 54 GDPR Rules on the establishment of the supervisory authority**

1. Each Member State shall provide by law for all of the following:
  - a. The establishment of each supervisory authority;
  - b. The qualifications and eligibility conditions required to be appointed as member of each supervisory authority;
  - c. The rules and procedures for the appointment of the member or members of each supervisory authority;
  - d. The duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24<sup>th</sup> May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
  - e. Whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
  - f. The conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits



incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

### **Suitable Recitals**

(117) Establishment of supervisory authorities; (121) Independence of the supervisory authorities.

### **COMMENTARY:**

As already indicated, the Directive says very little about the terms of appointment and the status applicable to the members of the supervisory authority as well as the modes for establishment of the supervisory authorities; at most, Article 28 (7) of the Directive imposed an obligation on the Member States to ensure that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 54 – Rules on the establishment of the supervisory authority Article 54(1) requires member states to “provide by law” for the “establishment of the supervisory authority,” including qualifications and eligibility conditions, rules and procedures, duration of and number of eligible terms, and obligations regarding appointment as a member of the supervisory authority.

## **Section 2: Competence, task and powers**

### **Art. 55 GDPR Competence**

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

### **Suitable Recitals**

(122) Responsibility of the supervisory authorities.

**COMMENTARY:**

Article 55 begins by restating the rule contained in Article 28, paragraphs 1 and 3, of the Directive that each supervisory authority shall be competent for the performance of the tasks assigned and the exercise of the powers conferred on it. In its first version, Article 55 of the draft Regulation also provides a new competence, that of lead authority when the controller or the processor is established in several Member States, in order to ensure uniform application ("single window").

This new competence of the lead supervisory authority is now subject to a specific provision in Article 56 and will therefore be discussed under that provision. It was already noted that Article 55 makes Article 56 inapplicable where the processing is carried out by public authorities or private bodies acting on the basis of article 6, paragraph 1, point (c) (i.e. when the processing is necessary for compliance with a legal obligation to which the controller is subject) or (e) (i.e. when the processing is necessary for the performance of a task in the public interest or in the exercise of public authority which is vested to the controller). In this case, the supervisory authority of the Member State concerned remains responsible.

Finally, pursuant to the terms of paragraph 3 of Article 55, the courts acting in their judicial capacity are not subject to the competence of the supervisory authorities to supervise processing operations but they shall still apply the material rules relating to the data protection. The question of the competence of the national supervisory authority was already addressed by Article 28, paragraphs 1 and 3, of the Directive. Accordingly, each supervisory authority shall have all the powers conferred on it in the territory of the relevant Member State, in order to ensure the compliance with the data protection rules of that territory. Pursuant to this provision, each national authority is territorially competent to exercise its powers in accordance with the procedural law of the relevant Member State, whatever the national law applicable to the processing in question.

**Art. 56 GDPR Competence of the lead supervisory authority**

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall

decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

### **Suitable Recitals**

(124) Lead authority regarding processing in several Member States; (127) Information of the supervisory authority regarding local processing; (128) Responsibility regarding processing in the public interest.

### **COMMENTARY:**

Lead supervisory authority is the authority with the primary responsibility for dealing with a cross-border data processing activity, for example when a data subject makes a complaint about the processing of his or her personal data. The lead supervisory authority will coordinate any investigation, involving other 'concerned' supervisory authorities. Identifying the lead supervisory authority depends on determining the location of the controller's 'main establishment' or 'single establishment' in the EU.

The concept of a concerned supervisory authority is meant to ensure that the 'lead authority' model does not prevent other supervisory authorities having a say in how a matter is dealt with when, for example, individuals residing outside the lead authority's jurisdiction are substantially affected by a data processing activity. In terms of factor (a) above, the same considerations as for identifying a lead authority apply. Note that in (b) the data subject must merely reside in the Member State in question; he or she does not have to be a citizen of that state. It will generally be easy – in (c) to determine – as a matter of fact – whether a particular supervisory authority has received a complaint.

Article 56 GDPR provides that the lead supervisory authority for cross-border processing of data will be the authority that is competent to supervise the entity engaged in data processing of individuals in different countries or, the authority competent to supervise the main establishment of the data controller or processor in case this has different establishments in several Member States.

Article 56, paragraphs (2) and (5) of the GDPR provide for a concerned supervisory authority to take a role in dealing with a case without being the lead supervisory authority. When a lead supervisory authority decides not to handle a case, the concerned supervisory authority that informed the lead shall handle it. This is in accordance with the procedures in Article 61 (Mutual assistance) and Article 62 (Joint operations of supervisory authorities) of the GDPR.

### **Art. 57 GDPR Tasks**

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:
  - a. Monitor and enforce the application of this Regulation;
  - b. Promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
  - c. Advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
  - d. Promote the awareness of controllers and processors of their obligations under this Regulation;
  - e. Upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
  - f. Handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
  - g. Cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
  - h. Conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
  - i. Monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
  - j. Adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

- k. Establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
  - l. Give advice on the processing operations referred to in Article 36(2);
  - m. Encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
  - n. Encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
  - o. Where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
  - p. Draft and publish the requirements for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
  - q. Conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
  - r. authorise contractual clauses and provisions referred to in Article 46(3);
  - s. Approve binding corporate rules pursuant to Article 47;
  - t. Contribute to the activities of the Board;
  - u. Keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
  - v. fulfill any other tasks related to the protection of personal data.
2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form, which can also be completed electronically, without excluding other means of communication.
3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.
4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

### **Suitable Recitals**

(122) Responsibility of the supervisory authorities; (123) Cooperation of the supervisory authorities with each other and with the Commission; (132) Awareness-raising activities and specific measures; (133) Mutual assistance and provisional measures; (137) Provisional measures.

## COMMENTARY:

Supervisory authorities (also colloquially known as “Data Protection Authorities” or “DPAs”) are given competence “for the performance of the tasks assigned to and the exercise of the powers conferred on it” described in the GDPR on their national territory. Recital 122 tells us that this competence includes “processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing in its territory”.

In cases where the legal basis for processing, whether by a private body or a public authority, is a legal obligation, acting in the public interest or in the exercise of official authority, the ‘concerned’ authority has competence and the cross-border lead authority system is dis-applied. The language is rather obscure, but Recital 128 says that a supervisory authority has exclusive jurisdiction over both public authorities and private bodies acting in the public interest, which in either case are established on the supervisory authority’s territory. It is not clear whether this contemplates multiple establishments and is a means of excluding the one-stop shop or whether it gives exclusive jurisdiction to the home supervisory authority even if the processing is elsewhere in the EU.

This might have wide application to private sector bodies – e.g. financial institutions carrying out anti-money-laundering activities in relation to customers elsewhere in the EU than the home country. Supervisory authorities cannot exercise jurisdiction over courts acting in a judicial capacity. ‘Court’ is not defined and it is not entirely clear how far down the judicial hierarchy this rule will extend. A lead-authority system is set up to deal with cross-border processing (see section on co-operation and consistency between supervisory authorities for further information about this complex arrangement).

## Tasks

There is a very comprehensive list of tasks given to the supervisory authorities by Article 57 of the GDPR. There is no need to list them all, because the last on the list is “fulfill any other tasks related to the protection of personal data”. Supervisory authorities must therefore do anything that might reasonably be said to be about the “protection of personal data”. Some tasks are worth emphasizing. Supervisory authorities are to monitor and enforce the “application” of the GDPR and to promote awareness amongst the public, controllers and processors.

They are to advise their governments and parliaments on proposed new laws. Helping data subjects, dealing with and investigating complaints lodged by individuals or representative bodies, conducting investigations and especially co-operating with other supervisory authorities are all specifically mentioned, as is monitoring the development of technical and commercial practices in information technology. Supervisory authorities are to encourage the development of Codes of Conduct and Certification systems and they are to “draft and publish the criteria for accreditation” of certification bodies and those which monitor codes of conduct. Supervisory authorities cannot charge data subjects or Data Protection Officers for

their services; the GDPR is however silent on whether controllers and processors could be charged fees in respect of services they receive from supervisory authorities. Powers Article 58 of the GDPR lists the powers of the supervisory authorities to which Member States can add if they wish.

Many of the powers correspond to the specific tasks listed in Article 57 and do not need repeating. Worthy of mention are: ordering a controller or processor to provide information; conducting investigatory audits; obtaining access to premises and data; issuing warnings and reprimands and imposing fines; ordering controllers and processors to comply with the GDPR and data subjects' rights; banning processing and trans-border data flows outside the EU; approving standard contractual clauses and binding corporate rules.

The exercise of powers by a supervisory authority must be subject to safeguards and open to judicial challenge. Member States must give supervisory authorities the right to bring matters to judicial notice and "where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation". Presumably the existing variation in powers will continue in accordance with national law and procedure. Finally, supervisory authorities must produce annual reports. In summary, the competence, powers and tasks of supervisory authorities are a comprehensive listing of everything a supervisory authority must or might do. This is largely a predictable consolidation of existing practices with some innovations in individual Member States.

Pursuant to the Directive, each national supervisory authority was responsible for monitoring the application within its territory of the provisions transposing the Directive as adopted by the Member States (Article 28 (1)). On this basis, the application of the measures could be referred to the relevant national supervisory authority by any person for verification of the lawfulness of personal data processing or with any request relating to the protection of his or her rights and freedoms with regard to such processing (Article 28 (4)).

Those authorities should also be consulted on all proposed legislative, administrative or regulatory drafts relating to the protection of rights and freedoms of individuals with regard to personal data processing (Article 28 (2)).

## **Art. 58 GDPR Powers**

1. Each supervisory authority shall have all of the following investigative powers:
  - a. to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
  - b. to carry out investigations in the form of data protection audits;
  - c. to carry out a review on certifications issued pursuant to Article 42(7);

d. to notify the controller or the processor of an alleged infringement of this Regulation;

e. to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

f. To obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

a. To issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

b. To issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

c. To order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

d. To order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

e. To order the controller to communicate a personal data breach to the data subject;

f. To impose a temporary or definitive limitation including a ban on processing;

g. To order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

h. To withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

i. To impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

j. To order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

a. To advise the controller in accordance with the prior consultation procedure referred to in Article 36;



- b. To issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
  - c. To authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
  - d. To issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
  - e. To accredit certification bodies pursuant to Article 43
  - f. To issue certifications and approve criteria of certification in accordance with Article 42(5);
  - g. To adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
  - h. To authorise contractual clauses referred to in point (a) of Article 46(3);
  - i. To authorise administrative arrangements referred to in point (b) of Article 46(3);
  - j. To approve binding corporate rules pursuant to Article 47.
4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.
5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.
6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

### **Suitable Recitals**

(122) Responsibility of the supervisory authorities; (129) Tasks and powers of the supervisory authorities; (131) Attempt of an amicable settlement.

### **COMMENTARY:**

Article 28 of the Directive provided for two types of powers given to supervisory authorities: a power of consultation of the national authorities drawing up administrative measures or regulations relating to the protection of the rights and freedoms of individuals with regard to the personal data processing; effective powers of control expressed in investigative powers, effective powers of intervention and powers to engage in legal proceedings. However, A wide space for maneuvering was left to Member States so that eventually, the powers of national supervisory authorities could differ widely from one Member State to another.

The powers provided to the national supervisory authorities are considerable - including sanctions - and probably will change the relationship profoundly between them and the controllers or the processors, in particular, where the authorities were previously organized as mere advisory and conciliation bodies. Thus they acquire coercive powers similar to those of the administrative authorities such as the competition authorities, with the well-known fear that they generate for the enterprises. They are therefore established for the future as real "policemen" of the data protection.

This extension of powers will necessarily involve a dramatic strengthening of human and financial resources available to existing authorities if we are to prevent these from remaining a dead letter. This will certainly raise some reluctance from the Member States, but will undoubtedly allow for the protection to be taken much more seriously than at present. In any event, the status of these authorities may change profoundly and give them institutional importance that they did not have before. It should be noted that the Member States will retain discretion as to the application of fines to public authorities and organizations (see the comments on Article 83).

#### **Art. 59 GDPR Activity reports**

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

#### **COMMENTARY:**

An activity report is provided at regular intervals by the supervisory authorities.

\* \* \*

## **CHAPTER 7: COOPERATION AND CONSISTENCY**

### **Section 1: Cooperation**

#### **Art. 60 GDPR Cooperation between the lead supervisory authority and the other supervisory authorities concerned.**

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

### **Suitable Recitals**

(124) Lead authority regarding processing in several Member States; (125) Competences of the lead authority; (130) Consideration of the authority with which the complaint has been lodged.

### **COMMENTARY:**

While the lead authority is in charge of operations, under Article 60(1) GDPR the lead supervisory authority shall cooperate with the other supervisory authorities concerned in order to reach a consensus on actions to be taken. It may request assistance by other concerned supervisory authorities under Article 61 GDPR, and especially for purposes of carrying out investigations or monitoring the implementation of measures taken, may conduct joint operations in accordance with Article 62 GDPR. All supervisory authorities concerned exchange relevant information (Article 60(1) cl. 2 and (3) GDPR). Concerning a decision, it is for the lead supervisory authority to submit a draft to the other concerned supervisory authorities.

According to Article 60(3) GDPR, their views have to be taken duly into account. Further, the other concerned supervisory authorities may, within four weeks, express relevant and reasoned objections as provided by Article 60(4) GDPR. This term is defined in Article 4(24) GDPR as stating whether there is an infringement of the GDPR, whether the envisaged action is in accordance with the GDPR and clearly demonstrate the significance of risks incurred by the draft decision with data subjects' fundamental rights and freedoms or the free flow of personal data.

If the lead supervisory authority agrees with the objection, it has to submit a revised draft to the other concerned supervisory authorities, who then have to submit any objections within two weeks according to Article 60(5) GDPR.

If no objections are submitted within the prescribed period, a consensus is deemed to exist by Article 60(6) GDPR and all supervisory authorities concerned are bound by the decision. When the decision is adopted, it is for the lead supervisory authority to take action with regard to the controller or processor, while the supervisory authority to which a complaint was lodged has to inform the complainant according to Article 60(7) GDPR.

#### **Art. 61 GDPR Mutual assistance**

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

- a. It is not competent for the subject-matter of the request or for the measures it is requested to execute; or
- b. Compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken

in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

### **Suitable Recitals**

(123) Cooperation of the supervisory authorities with each other and with the Commission;(132) Awareness-raising activities and specific measures;(133) Mutual assistance and provisional measures.

### **COMMENTARY:**

Under the Directive, the Member States were already required to help each other to fulfill their tasks and ensure full compliance with the data protection rules. So, Article 28 (6) of the Directive provides for the supervisory authorities to mutually cooperate to the extent necessary for the performance of their duties, in particular by exchanging all useful information. It may request assistance by other concerned supervisory authorities under Article 61 GDPR, and especially for purposes of carrying out investigations or monitoring the implementation of measures taken, may conduct joint operations in accordance with Article 62 GDPR.

The mutual assistance procedure of Article 61 GDPR is supposed to contribute to consistent implementation and application of the GDPR. It especially concerns information requests and supervisory measures, for instance requests to carry out prior authorizations and consultations, inspections and investigations. Under Article 61(3) GDPR the use of information exchanged is expressly limited to the purpose for which it was requested. The requested supervisory authority has to submit the

information without undue delay, but no later than a month after the request according to Article 61(2) GDPR.

The requested supervisory authority may refuse requests only under Article 61(4) GDPR when it is not competent *Ratione Materiae* (subject matter jurisdiction) or the measures requested violate provisions of the GDPR, Union or national law which binds the requested supervisory authority. Any refusal to submit information has to be substantiated with reasons according to Article 61(5) GDPR. If the requested supervisory authority fails to act within the prescribed period, Article 60(8) GDPR authorizes the requesting supervisory authority to take provisional measures in its Member State.

### **Art. 62 GDPR Joint operations of supervisory authorities**

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused

damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

### **Suitable Recitals**

(126) Joint decisions; (134) Participation in joint operations.

### **COMMENTARY:**

Pursuant to Article 28 (6) of the Directive, each authority may be requested to exercise its powers by an authority of another Member State. However, the implementation of joint operations by several control authorities was not covered by the Directive.

### **Joint operations.**

The joint operations mechanism under Article 62 GDPR extends to investigations and enforcement measures and gives the supervisory authority of any Member State concerned a right to participate in such operations. Supervisory authorities are either invited by the competent supervisory authority or can request to participate according to Article 62(2) GDPR. If such a request is not granted within one month Article 62(7) GDPR provides that the other supervisory authorities may take provisional measures. In that case, as under Article 60(8) GDPR for the mutual assistance procedure, the urgency mechanism of Article 66 GDPR is then triggered. In a joint operation a supervisory authority may, in accordance with national law, grant investigative powers on a seconding supervisory authority or, if allowed by national law, authorize the seconding supervisory authority to exercise its powers as provided by Article 62(3) GDPR. Both modi are subject to the guidance and presence of members or staff of the host supervisory authority and subjects the supervisory authorities own members or staff to the national law of the host Member State. In turn, the host supervisory authority assumes responsibility for the actions of the supervisory authority acting in its Member State under Article 62(4) GDPR.



## Section 2: Consistency

### Art. 63 GDPR Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

#### Suitable Recitals

(135) Consistency mechanism.

#### COMMENTARY:

Consistency Mechanism. The Board is at the heart of the consistency mechanism set out in Articles 63 et seq. GDPR. In order to ensure consistent interpretation and application of the GDPR, the Board may issue non-binding opinions under Article 64 GDPR and binding decisions in accordance with Article 65 GDPR.

### Art. 64 GDPR Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

- a. Aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);
- b. Concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;
- c. Aims to approve the requirements for accreditation of a body pursuant to Article 41(3), of a certification body pursuant to Article 43(3) or the criteria for certification referred to in Article 42(5);
- d. Aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);
- e. Aims to authorise contractual clauses referred to in point (a) of Article 46(3); or
- f. Aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple

majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

- a. The members of the Board and the Commission of any relevant information, which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and
- b. the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the competent supervisory authority referred to in paragraph 1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

### **Suitable Recitals**

(136) Binding decisions and opinions of the Board.

### **COMMENTARY:**

While Article 64(1) GDPR provides a list of activities of the supervisory authorities where the Board gives an opinion – such as the list defining when a Data Protection Impact Assessments has to be carried out under Article 35(4) GDPR, standard protection clauses under Articles 46(2)(d) and 28(8) GDPR among others – it may also be approached by supervisory authorities, the chair of the Board or the Commission to examine any matter of general application or affecting more than one Member State under its second paragraph. This particularly concerns cases where a supervisory authority does not comply with its obligation to provide mutual

assistance under Article 61 GDPR or engage in joint operations as prescribed in Article 62 GDPR and detailed above. The opinions of the Board have to be issued within eight weeks, which may be extended by another six weeks depending on the complexity of the issues according to Article 64(3)

### **Art. 65 GDPR Dispute resolution by the Board**

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

a. Where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

b. Where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

c. Where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

### **Suitable Recitals**

(136) Binding decisions and opinions of the Board.

### **COMMENTARY:**

Article 65 creates a mechanism by which the European Data Protection Board may resolve any disputes among the DPAs. Decisions of the Board and decisions jointly agreed upon by lead and concerned supervisory authorities become binding.

In any case, the lead DPA must notify the accused controller or processor of any final decision, whereas the DPA where the complaint was originally lodged must notify the complainant. The complainant retains its right to an effective judicial remedy against a legally binding decision of a supervisory authority or where the supervisory authority fails to deal with a complaint or inform a data subject about the outcome of a case within three months. Additionally, under Article 83 the “exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.”

If the lead supervisory authority does not follow the objection or regards it as not relevant and reasoned, it has to apply the consistency mechanism and the Board has to adopt a binding decision according to Article 65(1)(a) GDPR.

As described above the Board adopts decisions according to Article 65(1) GDPR, when the lead supervisory authority does not follow objections of supervisory authorities concerned, regards them as irrelevant or unreasoned, when there are conflicting views on the main establishment of a controller or processor, or when the competent supervisory authority either fails to request an opinion of the Board or decides not to follow an opinion of the Board under Article 64 GDPR. Article 65(2)-(4) GDPR prescribes that all decisions are adopted with a two-thirds majority and generally within one month, which may be extended by six weeks.

If the Board fails to adopt a decision by that time the quorum is lowered to a simple majority for an additional two weeks. In the case of a split vote, the chair

decides. During the time of deliberation, the competent supervisory authority is barred from adopting its draft decision. As pointed out in Recital 142 GDPR decisions of the Board can be brought before the ECJ in an annulment action under Article 263 TFEU (Treaty on the Functioning of the European Union) by supervisory authorities, as they are addressees of these decisions.

### **Art. 66 GDPR Urgency procedure**

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

### **Suitable Recitals**

(137) Provisional measures; (138) Urgency procedure.

### **COMMENTARY:**

There is an urgency procedure provided by Article 66(1) GDPR, which allows the supervisory authority concerned to circumvent the consistency mechanism of Articles 63-65 GDPR under exceptional circumstances in cases with an urgent need to protect the rights and freedoms of data subjects and to adopt immediate provisional measures for its Member State. These measures have to specify a period of validity, which may not exceed three months. In order to have final measures adopted, the supervisory authority concerned may request an urgent opinion or decision of the Board. According to paragraph 4 urgent opinions and decisions have to be adopted within two weeks by a simple majority.

In the opposite case, where the supervisory authority concerned does not take measures although there is an urgent need to act in order to protect the rights and freedoms of data subject, any supervisory authority may request an urgent opinion or decision of the Board according to Article 66(3) GDPR.

### **Art. 67 GDPR Exchange of information**

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

### **COMMENTARY:**

The Directive already vested in the Commission the ability to adopt implementing acts, in the form of directly applicable measures, after consulting the Board, which is composed of representatives of the Member States within the meaning of article 31 (1). However, under the Directive, this ability was limited to the area of the transfer of data to third countries.

In the case of a non-compliant opinion, Article 31 (2), paragraph 4, requires the Commission to defer the application of the measures for a period of three months and refer to the Board that is ultimately competent to decide on the appropriateness of such measures.

## **Section 3: European data protection board**

### **Art. 68 GDPR European Data Protection Board**

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. <sup>3</sup>The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

### **Suitable Recitals**

(139) European Data Protection Board.

### **COMMENTARY:**

This article provides detail description regarding establishment of European Data Protection Board (EDPB). This article also provides general rules regarding the composition and functioning of EDPB. GDPR Article 68 establishes the European Data Protection Board and contains some general rules regarding the composition and functioning of it.

## **Art. 69 GDPR Independence**

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.
2. Without prejudice to requests by the Commission referred to in Article 70(1) and (2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

### **Suitable Recitals**

(139) European Data Protection Board.

### **COMMENTARY:**

According to article 69 the EDPB is an independent legal body of the Union and it does not seek permission from anybody, in the performance of its task or to exercise its powers. GDPR Article 69 emphasizes the independence of the European Data Protection Board, adding that in the performance of its tasks and exercise of its powers it doesn't seek nor take instructions for anyone.

## **Art. 70 GDPR Tasks of the Board**

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:
  - a. Monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;
  - b. Advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

- c. Advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
- d. Issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
- e. Examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
- f. Issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
- g. Issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
- h. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).
- i. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;
- j. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);
- k. draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;
- l. review the practical application of the guidelines, recommendations and best practices;
- m. issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);



- n. encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;
  - o. approve the criteria of certification pursuant to Article 42(5) and maintain a public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8) and of the certified controllers or processors established in third countries pursuant to Article 42(7);
  - p. approve the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies referred to in Article 43;
  - q. provide the Commission with an opinion on the certification requirements referred to in Article 43(8);
  - r. provide the Commission with an opinion on the icons referred to in Article 12(7);
  - s. provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.
  - t. issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;
  - u. promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;
  - v. promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;
  - w. promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.
  - x. issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and
  - y. maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.
2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

### **Suitable Recitals**

(136) Binding decisions and opinions of the Board; (139) European Data Protection Board.

### **COMMENTARY:**

Article 30 of the Directive already listed the tasks of the board of the Article 29 Working Party to the Commission, as well as the way the Board is called to contribute to the uniform application of the national transposition rules. These tasks logically include the ability of the Board to examine any question relating to the transposition of the Directive by the Member States, in order to ensure its uniform application.

Then, Article 30 (2) gave the Article 29 Working Party the task to provide advice to the Commission regarding the level of protection in the Community and in third countries, as well as on the codes of conduct developed at Community level. The Article 29 Working Party should also advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms.

In addition to these tasks, the Working Party should inform the Commission on any divergences between the laws or practices of Member States likely to affect the corresponding protection for persons with regard to the processing of personal data in the Union. The Working Party also had a general competence to adopt initiative for recommendations on any matter pertaining to the protection of personal data in the Union.

Article 30 allowed for a dialog between the Article 29 Working Party and the Commission, in order to prepare a report on the response given by the Commission to the recommendations made by the Article 29 Working Party. This report was communicated to Parliament and published. Finally, the Article 29 Working Party has the obligation to prepare an annual activity report on the status of the personal data protection in the Union and in third countries. This report was publicized and communicated to the Commission and the Parliament.

GDPR Article 70, as mentioned, describes the many tasks of the European Data Protection Board and it's a pretty long list so do check it out indeed. This article basically elaborates tasks of EDPB.

**Art. 71 GDPR Reports**

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.
2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

**COMMENTARY:**

Article 30 (6) of the Directive, required the Article 29 Working Party to draw up an annual report on the status of the protection of natural persons with respect to the personal data processing in the Community and in third countries. The report had to be published and communicated to the Commission, the European Parliament and the Council. GDPR Article 71 is about the duty of the EDPB to make an annual report on, among others, the personal data protection of data subjects where processing happens in the EU and, where relevant outside of the EU. The report is public.

**Art. 72 GDPR Procedure**

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.
2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

**COMMENTARY:**

Under the Directive, the G29 decisions should be taken by a simple majority of the representatives of the authorities within that Working Party. GDPR Article 72 simply says that when the EDPB takes decisions, normally it's by a simple majority of its members and in some cases by a two-thirds majority.

**Art. 73 GDPR Chair**

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

**COMMENTARY:**

GDPR Article 73 says that, again via a simple majority vote, each five years the European Data Protection Board elects a chair and two deputy chairs. These have to be members of the board and can only be re-elected once (so never one person more

than 10 years). The Article 29 Working Party was allowed to elect their chair for a term of 2 years. In addition, pursuant to the Directive, the chair mandate was renewable.

### **Art. 74 GDPR Tasks of the Chair**

**1.** The Chair shall have the following tasks:

1. to convene the meetings of the Board and prepare its agenda;
2. to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
3. to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

**2.** The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

### **COMMENTARY:**

GDPR Article 74 expands on what the tasks of the chair of the European Data Protection Board are with, on top of a list of tasks the additional stipulation that the allocation of tasks that need to be executed by the chair and deputy chairs must be in the rules of procedure. Under the Directive, the Chair's task was essentially to include in the agenda the matters to be considered by G29 (see Art. 29 (7)).

### **Art. 75 GDPR Secretariat**

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
6. The secretariat shall be responsible in particular for:
  - a. the day-to-day business of the Board;

- b. communication between the members of the Board, its Chair and the Commission;
- c. communication with other institutions and the public;
- d. the use of electronic means for the internal and external communication;
- e. the translation of relevant information;
- f. the preparation and follow-up of the meetings of the Board;
- g. the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

### **Suitable Recitals**

(140) Secretariat and staff of the Board.

### **COMMENTARY:**

Article 75 states that the Board secretariat shall be provided by the European Data Protection Supervisor and defines their tasks. In general, the secretariat shall provide analytical, administrative and logistical support to the Board. In order to ensure the independence of the secretariat, Article 75 provides various safeguards, including organizational such as all the tasks of the secretariat shall be carried out under the exclusive authority of the Chair of the European Data Protection Board. In addition, paragraph 3 imposes the organizational separation of the staff of the Board secretariat from that of the secretariat of the European Data Protection Supervisor, which implies that the Board secretariat must be subject to separate hierarchical relations, still intended to ensure its independence.

Paragraph 4 enables the Board, in conjunction with the European Supervisor, to establish and publish a Memorandum of Understanding applicable to the staff, implementing the aforementioned organizational separation and specifying the terms of cooperation between the Board and the European Supervisor. Paragraph 6 contains a list of the tasks entrusted to the secretariat, namely: the day-to-day business of the European Data Protection Board; the communication between the members of the Board, its Chair and the Commission and the communication with other institutions and the public.

The secretariat must also ensure the use of electronic means for internal and external communication as well as the translation of relevant information. Finally, the secretariat shall ensure the preparation and follow-up of the meetings of the European Data Protection Board and also the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board. Article 29 of the Directive stipulated that the Article 29 Working Party shall be assisted by a secretariat provided by the Commission.

**Art. 76 GDPR Confidentiality**

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.
2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council.

**COMMENTARY:**

GDPR Article 76, finally, provides a few words on confidentiality in the scope of discussions of the EDPB and access to documents. Article 76 expressly states that the discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure. Regulation (EC) shall govern access to documents submitted to members of the Board, experts and representatives of third parties No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. In its first version, paragraph 3 of Article 76 imposed on the Chair the requirement to ensure that the members of the Board, the experts and the representatives of third parties are made aware of their duty to comply with the rule of confidentiality. However, this provision has not been maintained. The Directive did not provide for confidentiality of the discussions of the Article 29 Working Party.

\* \* \*

## **CHAPTER 8: REMEDIES, LIABILITY AND PENALTIES**

### **Art. 77 GDPR Right to lodge a complaint with a supervisory authority**

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.
2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

#### **Suitable Recitals**

(141) Right to lodge a complaint.

#### **COMMENTARY:**

The GDPR says that data subjects can lodge a complaint with a supervisory authority if they believe that the processing of their data infringes the GDPR. The complaint must be lodged with the supervisory authority of the EU member state where the data subject has their habitual residence or place of work, or of the member state where the alleged infringement occurred. In the event that a supervisory authority does not inform a data subject about the progress or outcome of their complaint within three months, or partially or wholly rejects or dismisses the complaint, the data subject shall have the right to an effective judicial remedy.

The Directive already required Member States to implement a procedure for lodging a complaint with the supervisory authority. Thus any person or an association representing that person may lodge a complaint concerning the protection of his or her rights and freedoms in regard to the processing of personal data. This may in particular consist of a request for verification of the lawfulness of processing. Pursuant to Article 28 (4), the person concerned shall be informed of the outcome of the claim or that a check has taken place. In countries where the authority had no decision-making power, an increase in complaints may be expected, as this situation will lead to a decision likely to be appealed. The problem is then to determine what will be the procedure before the national authority, which should not be overly complicated and/or costly as this may discourage the data subject from pursuing a complaint.

### **Art. 78 GDPR Right to an effective judicial remedy against a supervisory authority**

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority, which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

### **Suitable Recitals**

(141) Right to lodge a complaint; (143) Judicial remedies.

### **COMMENTARY:**

The Regulation goes further than the Directive: it is not at the discretion of Member States to set up a procedure for appeals, but an absolute right granted to any physical person or legal entity to appeal against a legally binding decision of the supervisory authority concerned. The right to a judicial remedy against a decision by a supervisory authority is an essential element of the protection of individuals with regard to the processing of personal data. This right to a an effective judicial remedy arises where the supervisory authority does not handle a complaint or does not inform the data subject within three months or a shorter period as prescribed by the applicable national law, on the progress or outcome of the complaint lodged.

As a principle, the data subject must lodge a complaint in the jurisdiction of the Member State where the supervisory authority is established. Finally, the European text obliges the supervisory authority to communicate to the relevant jurisdiction a complaint against one of its decisions, the notice or the decision of the European Data Protection Board, which would have been made previously under the consistency mechanism.

We have seen in Article 77 that pursuant to the Directive, the Member States should implement a procedure whereby any citizen, or an association that represents that citizen can lodge a complaint with the competent control authority, especially to check the lawfulness of a relevant processing. The Directive further provided that decisions by the supervisory authorities, which give rise to complaints may be appealed through the courts.

The evolution is significant. Several States did not allow an appeal against the decisions of the supervisory authorities, often due to their lack of binding powers. The states should therefore insert this remedy in their domestic law, according to their specific procedures (administrative, judicial courts, etc.).



## **Art. 79 GDPR Right to an effective judicial remedy against a controller or processor**

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

### **Suitable Recitals**

(141) Right to lodge a complaint; (145) Choice of venue.

### **COMMENTARY:**

Article 79 gives people affected by processing, a genuine right to an effective judicial remedy against both the controller and the processor in case of infringement of their rights resulting from the processing of their data. This right is not to be confused either with the possibility of lodging a complaint with a supervisory authority referred to in article 78, nor with any other administrative or extra-judicial remedy provided under the relevant national law. The second paragraph allows the data subject to bring his action either before the courts of the Member State in which the controller has an establishment or in the courts of the state of habitual residence of the data subject, unless controller or processor is a public authority of a Member State acting in the exercise of its public powers.

It should be noted that as per recital 146, the jurisdictional rules contained in the Regulation need subject to the general jurisdictional rules contained in other legal instruments, such as those contained in Regulation (EU) No. 1215/2012 of the European Parliament and the Council of 12 December 2012 concerning jurisdiction, recognition and enforcement of decisions on civil and commercial matters. The Directive Article 22 requires the Member States to provide to any person the right to a judicial remedy in case of breach of the rights guaranteed to him by the national provisions transposing the Directive.

### **Individuals have the following rights (against controllers and processors):**

- the right to lodge a complaint with supervisory authorities where their data have been processed in a way that does not comply with the GDPR;

- the right to an effective judicial remedy where a competent supervisory authority fails to deal properly with a complaint;
- the right to an effective judicial remedy against a relevant controller or processor; and
- the right to compensation from a relevant controller or processor for material or immaterial damage resulting from infringement of the GDPR.
- Both natural and legal persons have the right of appeal to national courts against a legally binding decision concerning them made by a supervisory authority.
- Individuals can bring claims for non-pecuniary loss, not just for compensation. The potential for group actions to be brought is facilitated.
- Judicial remedies and liability for compensation extend to both data controllers and data processors who infringe the Regulation.

### **Art. 80 GDPR Representation of data subjects**

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that anybody, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

### **Suitable Recitals**

(142) The right of data subjects to mandate a not-for-profit body, organisation or association.

### **COMMENTARY:**

Article 80 specifies and supplements the Directive regarding option for representation by an association. The Regulation provides that an association (non-profit association active in the protection of the rights of the data subjects) can be mandated by a data subject not only to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77 on his or her behalf, but also for judicial remedy against a decision of a supervisory authority (Article 78) or against a controller or a processor (see Article 79).

The final version of the Regulation adds that the association is also granted the right to claim compensation as provided by Article 82 on behalf of the data subject where he or she considers that his or her rights under this Regulation have been infringed and as provided by Member State law. The Member States may grant major powers of action to the associations charged with the protection of rights and freedoms in the data processing. If the state makes use of this provision, these associations may, at their initiative (i.e., regardless of any mandate by a data subject) lodge a claim with a supervisory authority in the territory of the Member State of their establishment (Art. 77) or expedite a judicial remedy against a decision of a supervisory authority (Article 78) or against a controller or a processor (Article 79) if they consider that the rights of a data subject have breached because the personal data processing has not been compliant with the Regulation.

The Directive already provided for the possibility of an association undertaking to lodge a complaint with a supervisory authority on behalf of a person complaining of a breach of his or her rights and freedoms in the context of the personal data processing. It is a fundamental principle, that associations have the recognized powers to defend of the rights of data subjects. We strongly believe this measure will contribute to ensuring the effectiveness of the rights granted to the data subjects by the personal data processing.

Jurisdictional procedures already exist for data subjects; however, it is very rare that a person resorts to legal proceedings, especially in view of the costs. In other words, at present, it is not worth the effort. However, this development could lead to many problems of implementation. Regarding the possibility for these associations introducing a procedure regardless of a mandate by the data subject, it is not possible to predict the future implications in different Member states and disparities in the protection of the data subjects will appear on this point. Associations must exist and be active regarding data protection, but will often involve a significant change in attitudes of the public, members and authorities.

Data subjects can allow not-for-profit bodies, organisations or associations to act on their behalf by lodging complaints, receiving compensation and exercising some rights with regard to complaints and judicial remedies. These entities can also have the right to act independently of a data subjects' mandate if the Member States provide for this possibility.

### **Art. 81 GDPR Suspension of proceedings**

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.
2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

### **Suitable Recitals**

(144) Related proceedings.

### **COMMENTARY:**

Where a court in one Member State learns of proceedings pending in another Member State, concerning the same controller or processor and the same subject matter, that court may:

- contact the relevant court in the other Member State to confirm the existence of such proceedings; and
- suspend its own proceedings if appropriate.

Where these proceedings are pending at first instance, any other court may also, on the application of one of the parties, decline jurisdiction, if the court first seized has jurisdiction.

## **Art. 82 GDPR Right to compensation and liability**

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

### **Suitable Recitals**

(146) Indemnity; (147) Jurisdiction.

### **COMMENTARY:**

Article 82 of the Regulation confirms the above, by specifying the principle of compensation for the material or immaterial damage suffered by any person as a result of an infringement of this Regulation. The compensation may be received from the “controller” or the “processor”. Paragraph 2 of this provision also specifies the events giving rise to the liability of both participants: that a processor shall be liable for its “participation in processing” while the processor shall be only liable for failure to perform the obligations specifically imposed by the Regulation or where it has acted outside or contrary to lawful instructions of the controller.

Exemption from the Directive is applicable in favour of the two actors if proven that the event, which caused the damage is not attributable to it. The real novelty of this provision involves the establishment of a joint liability of the controller(s) and/or the processor(s) involved in the same processing under the conditions defined by the provision. To this end, either the controllers or the processors, or the controller or the processor involved in the same processing must be held liable for damage caused by the processing pursuant to paragraphs 2 and 3. In this case, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

Court proceedings for exercising the right to receive compensation shall be brought before the courts designated competent under the law of the Member State referred to in Article 79 (2). Article 23 of the Directive provided for the right to receive from the controller compensation for the damage suffered as a result of an unlawful processing operation or of any act incompatible with said Directive. A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage (fault of the data subject, force majeure, etc.).

This provision implied that a legal remedy is available under national legislation (recital 55).

### **Art. 83 GDPR General conditions for imposing administrative fines**

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- a. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- b. the intentional or negligent character of the infringement;
- c. any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- d. the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- e. any relevant previous infringements by the controller or processor;
- f. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- g. the categories of personal data affected by the infringement;
- h. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- i. where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- j. adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- a. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
- b. the obligations of the certification body pursuant to Articles 42 and 43;
- c. the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- a. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- b. the data subjects' rights pursuant to Articles 12 to 22;
- c. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- d. any obligations pursuant to Member State law adopted under Chapter IX;
- e. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall

notify to the Commission the provisions of their laws, which they adopt pursuant to this paragraph by 25<sup>th</sup> May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

### **Suitable Recitals**

(148) Penalties; (149) Penalties for infringements of national rules; (150) Administrative fines; (151) Administrative fines in Denmark and Estonia; (152) Power of sanction of the Member States.

### **COMMENTARY:**

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 and presented below:

These fines must be in all cases effective, proportionate and dissuasive.

Depending on the circumstances of each individual case, the fines shall be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58 (2) that may be imposed by the supervisory authority.

When deciding on the amount of the administrative fine in each individual case, the authority must give due regard to the following:

- a. the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- b. the intentional or negligent character of the infringement;
- c. any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- d. the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 (protection by design and protection by default) and 32 (security of processing);
- e. any relevant previous infringements by the controller or processor;
- f. the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- g. the categories of personal data affected by the infringement;
- h. the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- i. Where measures have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures.
- j. Regard should also be given to the adherence to approved codes of conduct or approved certification mechanisms;



k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

As to the amounts, a gradual system exists depending on the severity attributed to the infringement:

1. Administrative fines up to EUR 10,000,000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (paragraph 4):

a. the obligations of the controller and the processor:

- relating to consent of children in connection with information society services (Art. 8);
- relating to processing not requiring identification (Art. 11);
- relating to data protection by design and data protection by default (Art. 25);
- rules specific to the joint controllers (Art. 26);
- relating to representatives of the controller not established in the Union (Art. 27);
- imposed in the relationship between the controller and the processor (Art. 28);
- relating to processing under the authority of the controller or processor (Art. 29);
- relating to keeping a register of all categories of processing activities (Art. 30);
- concerning the cooperation with the supervisory authority (Art. 31);
- regarding to the security of processing (Art. 32);
- relating to the notification of data breach to the supervisory authority (Art. 33);
- relating to the notification of data breach to the data subjects (Art. 34);
- concerning the impact assessment regarding the data protection (Art. 35) and prior consultation of the supervisory authority (Art. 36);
- concerning the designation of a data protection officer (Art. 37), its functions (Art. 38), its missions (Art. 39);
- relating to certification (Art. 42) and the certification procedure (Art. 43).

b. obligations of the certification body in the meaning of Articles 42 and 43;

c. obligations of the body charged to monitor the adherence to the code of conduct in the meaning of Art. 41 (4)

1. Fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements to the following provisions (paragraph 5):

- the basic principles for processing, including conditions for consent, pursuant to Articles 5 (Principles relating to processing of personal data), 6 (Lawfulness of

processing), 7 (Conditions applicable to consent) and 9 (Processing of specific categories of personal data);

- the rights of data subjects within the meaning of Articles 12 to 22 of the Regulation;

- rules relating to the transfers of personal data to a recipient in a third country or an international organization (Articles 44 to 49);

- any obligations pursuant to Member State law adopted under Chapter IX; let's remind that Chapter IX gives the Member States a certain discretion in view of processing of personal data and freedom of expression and information (see Art. 86); processing of a national identification number (Art. 87), etc.

- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58 (2) or failure to provide access in violation of Article 58 (1);

In addition, non-compliance with an order by the supervisory authority shall be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. It should be noted that if a controller or processor intentionally or negligently, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58 (2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

Finally, where the legal system of the Member State does not provide for administrative fines, Article 83 may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts. In this case, those legal remedies must be effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In all cases, those fines must be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt not later than the day of entry of this Regulation into force pursuant to Article 99 (2) and also notify without delay any subsequent amendment law or amendment affecting them.

Directive relied totally on Member States regarding the sanctions in case of violation of provisions adopted in application of the Directive (Article 24).

The most obvious difficulty will be for recognition by each Member States legal system of such new powers to be exercised by the supervisory authorities and to provide specific procedural safeguards to be implemented in addition to the general

procedural rules. In Belgium for example, the possible recognition of such a power to impose fines of such an amount would change completely the relationship of individuals to the Commission for Protection of Privacy. The latter, as we have said, was designed more as a conciliatory body than a controlling authority and previously had no power to impose any fines. It should be noted that the power of the national authority could be limited to the initiation of the fine and only a court would have the competence to impose it. The questions are what the initiation power would cover and whether the court may or may not review or refuse to apply it in the context of its intervention.

### **Art. 84 GDPR Penalties**

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements, which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law, which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### **Suitable Recitals**

(149) Penalties for infringements of national rules; (150) Administrative fines; (151) Administrative fines in Denmark and Estonia; (152) Power of sanction of the Member States.

### **COMMENTARY:**

Member States set their own rules on penalties applicable to infringements of the GDPR, in particular those infringements that are not subject to administrative fines. Member States may also provide their own rules on criminal sanctions for infringement of the GDPR. The Directive contained only a general provision (Art. 24) requiring the states to take appropriate measures to ensure full implementation of its provisions and specify penalties in cases of infringement of the provisions adopted pursuant to this Directive.

\* \* \*

## **CHAPTER 9: PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS**

### **Art. 85 GDPR Processing and freedom of expression and information**

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.
2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

#### **Suitable Recitals**

(153) Processing of personal data solely for journalistic purposes or for the purposes of academic, artistic or literary expression.

#### **COMMENTARY:**

This provision requires Member States to introduce exemptions to the GDPR where necessary. Although this Article is wider in scope than Article 9 of the Data Protection Directive, Article 85 makes special provision for processing carried out for journalistic purposes, or for the purposes of academic, artistic or literary expression. Member States will be required to notify the Commission on how they have implemented this requirement and of any changes to such laws. The Directive already allowed Member States to provide for exemptions or derogations for personal data processing carried out solely for journalistic, artistic or literary expression, from the general conditions of lawfulness of processing (Chapter II), from the conditions of data transfer to third countries (Chapter IV) and from the competence of the supervisory authorities (Chapter VI) only insofar as they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

### **Art. 86 GDPR Processing and public access to official documents**

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to

official documents with the right to the protection of personal data pursuant to this Regulation.

### **Suitable Recitals**

(154) Principle of public access to official documents.

### **COMMENTARY:**

Personal data contained in official documents may be processed, in order to reconcile public access to official documents with the right to the protection of personal data. This provision expands on Recital 72 of the Data Protection Directive, and allows personal data within official documents to be disclosed in accordance with Union or Member State laws, which allow public access to official documents. This is not without limit - such laws should, according to Recital 154 GDPR. Directive 2003/98/EC (the “PSI Directive”) on the “re-use of public sector information” does not alter the obligations on authorities, or rights of individuals, under the GDPR.

### **Art. 87 GDPR Processing of the national identification number**

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

### **COMMENTARY:**

Member States are free to determine the conditions under which national ID numbers may be processed, subject to appropriate safeguards for the rights and freedoms of data subjects pursuant to the GDPR. This effectively replicates the right of Member States to set their own conditions for processing national identification numbers under the Data Protection Directive. The only expansion is to clarify that this requires appropriate safeguards to be put in place.

Pursuant to Article 8 (7) of the Directive, the Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed. An example is that Belgian and French legislatures have adopted specific laws governing the consultation and the use of the National Register of Natural Persons, of the National Repertory of Identification of Natural Persons (RNIPP).

### **Art. 88 GDPR Processing in the context of employment**

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the

purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law, which it adopts pursuant to paragraph 1, by 25<sup>th</sup> May 2018 and, without delay, any subsequent amendment affecting them.

### **Suitable Recitals**

(155) Processing in the employment context.

### **COMMENTARY:**

Member States may create new laws or conclude collective agreements to ensure the protection of personal data in the context of national employment law. These must include appropriate safeguards. Member States must inform the Commission of any laws adopted in this area.

Member States are permitted to establish (either by law or through collective agreements) more specific rules in respect of the processing of employee personal data, covering every major aspect of the employment cycle from recruitment to termination. This includes the ability to implement rules setting out when consent may be deemed valid in an employment relationship. Such rules must include specific measures to safeguard the data subject's "*dignity, legitimate interests and fundamental rights*" and the GDPR cites transparency of processing, intragroup transfers and monitoring systems as areas where specific regard for these issues is required. Member States must notify the Commission of any laws introduced under this Article by the time the GDPR enters into force, and must also notify it of any amendments.

### **Art. 89 GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational

measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing, which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

### **Suitable Recitals**

(156) Processing for archiving, scientific or historical research or statistical purposes; (157) Information from registries and scientific research; (158) Processing for archiving purposes; (159) Processing for scientific research purposes; (160) Processing for historical research purposes; (161) Consenting to the participation in clinical trials; (162) Processing for statistical purposes; (163) Production of European and national statistics.

### **COMMENTARY:**

Subject to appropriate safeguards, and provided that there is no risk of breaching the privacy of the data subject, Member States may restrict the data subject's rights to access, rectification, restriction of processing and to object when it comes to the processing of their personal data for scientific, historical or statistical purposes.

Article 89(1) acknowledges that controllers may process data for these purposes where appropriate safeguards are in place (see section on lawfulness of processing and further processing and sensitive data and lawful processing). Where possible, controllers are required to fulfill these purposes with data which does not permit, or no longer permits, the identification of data subjects; if anonymisation is not possible, pseudonymization should be used, unless this would also prejudice the purpose of the research or statistical process.

Article 89(2) allows Member States and the EU to further legislate to provide derogations from data subject rights to access, rectification, erasure, restriction and objection (subject to safeguards as set out in Article 89(1)) where such rights “*render impossible or seriously impair*” the achievement of these specific purposes, and derogation is necessary to meet those requirements.

The recitals add further detail on how “*scientific research*”, “*historical research*” and “*statistical purposes*” should be interpreted. Recital 159 states that scientific research should be “*interpreted in a broad manner*” and includes privately funded research, as well as studies carried out in the public interest. In order for processing to be considered statistical in nature, Recital 162 says that the result of processing should not be “*personal data, but aggregate data*” and should not be used to support measures or decisions regarding a particular individual.

The Directive already provided various exemptions from the principles of protection for processing for historical, statistical or scientific purposes. For example, Article 6 already provided that such processing was not deemed incompatible with various initial purposes, subject to safeguards under national law. Under the same condition, the data could also be stored longer than necessary for the initial purpose or even for a purpose deemed to be compatible. Still with appropriate safeguards, Article 11 (2) provided an exemption from the obligation to notify data subjects about processing for such purposes if the notification to the data person would be impossible or would imply disproportionate effort or if the legislation explicitly provided for data recording or communication.

Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States might, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data is processed solely for purposes of scientific research or are kept in a personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics (Article 13 (2)).

## **Art. 90 GDPR Obligations of secrecy**

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.



2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

### **Suitable Recitals**

(164) Professional or other equivalent secrecy obligations.

### **COMMENTARY:**

Member States may create their own rules in relation to controllers or processors that are subject to obligations of professional secrecy. Member States that adopt such rules must inform the Commission. This Article allows Member States to introduce specific rules to safeguard “*professional*” or “*equivalent secrecy obligations*” where supervisory authorities are empowered to have access to personal data or premises. These rules must “*reconcile the right to protection of personal data against the obligations of secrecy*”, and can only apply to data received or obtained under such obligation. Again, Member States must notify the Commission of any laws introduced under this Article by the time the GDPR enters into force, and must also notify it of any amendments.

## **Art. 91 GDPR Existing data protection rules of churches and religious associations**

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfills the conditions laid down in Chapter VI of this Regulation.

### **Suitable Recitals**

(165) No prejudice of the status of churches and religious associations.

### **COMMENTARY:**

Where, in a Member State, churches and religious associations or communities impose rules regarding the processing of personal data, such rules may continue to apply, provided that they are brought into line with the provisions of the GDPR. Churches and religious associations that impose such rules are subject to the oversight of the relevant DPA.

This Article protects “*comprehensive*” existing rules for churches, religious associations and communities where these are brought into line with the GDPR’s provisions. Such entities will still be required to submit to the control of an

independent supervisory authority under the conditions of Chapter VI (see section on co-operation and consistency between supervisory authorities).

\* \* \*

## CHAPTER 10: DELEGATED ACTS AND IMPLEMENTING ACTS

### Art. 92 GDPR Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.
3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

### Suitable Recitals

(166) Delegated acts of the Commission; (167) Implementing powers of the Commission; (168) Implementing acts on standard contractual clauses; (169) Immediately applicable implementing acts; (170) Principle of subsidiarity and principle of proportionality.

### COMMENTARY:

In order to fulfill the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardized icons and procedures for providing such icons. It is of particular importance that the Commission carries out appropriate consultations during its preparatory work, including at expert level.

The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on

the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organization; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organization does not ensure an adequate level of protection, and imperative grounds of urgency so require.

### **Art. 93 GDPR Committee procedure**

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation ((EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

### **COMMENTARY:**

Let's recall that several provisions of the Regulation grant implementing competency to the Commission concerning, for example, approval of codes of conduct (Article 40 (9)); the definition of technical standards for the certification mechanisms (Article 43 (9)); decisions relating to the adequate nature of the level of protection in a non-EU third country (Article 44 (3)); the adoption of standard clauses for data protection (Article 46 (2), (c)). Each of the provisions conferring implementing powers to the Commission provides that the implementing acts should be adopted in accordance with the procedure referred to in article 93 (2) or, in an extreme urgency, in accordance with the procedure laid down in article 93 (3).

Article 93 refers to Article 5 or Article 8 of Regulation (EU) No. 182/2011 of Regulation (EU) No. 182/2011 of the European Parliament and the Council of 16 February 2011 establishing the rules and general principles on the modes of control by the Member States of the exercise of the powers of enforcement by the Commission, depending on whether the future Regulation refer to paragraphs 2 or 3

of article 87. Regulation 181/2011 sets out the procedure to follow when a legally binding Union act requires uniform conditions of implementation and that the implementing acts by the Commission are submitted to the control of the Member States.

Article 5 of that Regulation defines the procedure of review:

- The Chair of the Committee (committee composed of representatives of the Member States) responsible for assisting the Commission shall submit a draft-implementing act to the Committee;
- The Committee shall issue an opinion by a qualified majority (qualified majority is defined in article 16 (4) of the Treaty on the European Union as being equal to at least 55% of the members of the Council, comprising at least fifteen of them and representing Member States with at least 65% of the population of the Union);
- In the case of a favourable opinion of the Committee, the Commission shall adopt the draft-implementing act;
- in the case of an unfavourable opinion , two cases are possible: the Chair can either submit a modified version of the draft implementing act to the same Committee, within a period of two months from the issue of the unfavourable opinion, or submit draft implementing act, within a period of one month from the issuance of this opinion, to a Committee of appeal for a new discussion.
- in the absence of an opinion of the Committee, the Commission can, in principle, adopt the draft implementing act.

As previously indicated, certain provisions of the Regulation provide that for reasons of urgency, said implementing acts should be adopted in accordance with paragraph 3 of Article 93, which on this part refers to Article 8 of Regulation 181/2011. According to this provision, an implementing act can apply immediately, without needing to be previously submitted to a Committee, for duly justified reasons of extreme urgency. In this case, the implementing act remains in force only for a period of six months. It is the responsibility of the Chair however to submit the implementing act to the Commission for review, not later than fourteen days after its adoption. In case of negative opinion, the Commission shall immediately repeal the act.

\* \* \*

## **CHAPTER 11: FINAL PROVISIONS**

### **Art. 94 GDPR Repeal of Directive 95/46/EC**

1. Directive 95/46/EC is repealed with effect from 25<sup>th</sup> May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

#### **Suitable Recitals**

(171) Repeal of Directive 95/46/EC and transitional provisions.

#### **COMMENTARY:**

Logically, Article 94 repeals the Directive from the moment when the Regulation enters into force that is 2 years after the 20th day following its publication in the Official Journal of the European Union. The Regulation does not affect the decisions of the Commission, which were adopted on the basis of the Directive, and the permissions that have been granted by the supervisory authorities on the basis of Directive 95/46/EC. The GDPR repeals the Directive, with effect from the GDPR Effective Date. From that point on, any references to the Directive will be construed as references to the GDPR, and any references to the WP29 will be construed as references to the EDPB.

### **Art. 95 GDPR Relationship with Directive 2002/58/EC**

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

#### **Suitable Recitals**

(173) Relationship to Directive 2002/58/EC.

#### **COMMENTARY:**

Article 95 clarifies the link with Directive 2002/58/EC of 12<sup>th</sup> July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. The Regulation does not impose any additional obligations in the provision of electronic communications services available to the public on public networks of communications in the Union, for the areas in which they are submitted to specific obligations having the same purpose as those set out in Directive 2002/58/EC.

According to recital 173, the future Regulation is intended to apply to all aspects of the protection of rights and freedoms with respect to the personal data processing,

unless specific obligations with the same purpose are set out in the Directive 2002/58/EC. The Regulation calls for a revision of Directive 2002/58/EC to ensure consistency with the new European text. The GDPR does not impose additional obligations on telecoms providers that process personal data under the e-Privacy Directive. However, there remains some uncertainty in the relationship between the e-Privacy Directive and the GDPR, which will require future clarification.

### **Art. 96 GDPR Relationship with previously concluded Agreements**

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

#### **COMMENTARY:**

International agreements involving the transfer of personal data to third countries or international organizations which were concluded by Member States prior to the entry into force of the GDPR, and which are compliant with applicable EU law remain in force until amended, replaced or revoked.

### **Art. 97 GDPR Commission reports**

1. By 25<sup>th</sup> May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:
  - a. Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
  - b. Chapter VII on cooperation and consistency.
3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

**COMMENTARY:**

The Directive was already requiring the Commission to provide a report to the European Parliament and the Council on the application of the Directive, accompanied, as appropriate, by proposals for amendment (see Article 33).

**Art. 98 GDPR Review of other Union legal acts on data protection**

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

**COMMENTARY:**

In the final version of the Regulation, a new provision was included in Article 98 relating to the review of other legal instruments on the data protection occurring in the Union. Pursuant to this new provision, the Commission is granted the power to submit legislative amendments to any other legal instruments under EU law on data protection. The goal is to ensure, by means of amendments, the consistency of the protection of individuals with respect to the personal data processing, particularly with regard to the protection of individuals with respect to the processing carried out by the European institutions (see Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of natural persons with respect to the treatment of the personal data by the Community institutions and bodies) and the free movement of such data).

**Art. 99 GDPR Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. It shall apply from 25<sup>th</sup> May 2018.

**COMMENTARY:**

Article 99 specifies that this Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. The Regulation was published on 4<sup>th</sup> May 2016 in the Official Journal of the European Union and will therefore enter into force on 25<sup>th</sup> May 2016. However, the Regulation will only be applicable after the two years following its entry into force, i.e., from 25<sup>th</sup> May 2018 on. The Regulation does not provide for a transitional regime, but, strangely, gives some transition principles in recital 171. Thus, any processing operations in progress at the time of the entry into force of the Regulation on 25<sup>th</sup> May 2016 will have to be brought into line within a period of two years.



It further provides that the consent given under the Directive should not be repeated, as it was given in accordance with the terms of the settlement so that the controller can continue such processing after the date of entry into force of the Regulation. We may wonder what the purpose of such a rule is. In a previous version, it was stated "Where such processing is in line with Directive 95/46/EC, it is not necessary that the data subjects agrees again to allow the controller to continue processing after the date of application of this Regulation". We see that the recital does not provide for anything new: the consent which was given by a data subject earlier and which was given consistent with the Regulation should not be repeated, which had been assumed.

Finally, Article 99 reminds the mandatory character of all the elements contained in the Regulation and its directly binding character in all Member States.

The lack of a transitional regime is problematic, for example, when considering the impact analyses that must precede the implementation of certain processing operations or the prior consultation of the supervisory authority. Will the rendering of compliance with the existing processing operations result in the need for retroactive analyses or prior consultations? The second version of the Regulation provided explicitly for these scenarios, incorporating an exemption if the processing was consistent with the Directive, but this was erased in the final version.

Such seems to be the extreme consequences, which the system of rendering the processing operations into compliance results in – and is provided for in one recital only. In addition to the questions that may be asked on the nature of such a “rule” that is provided for in the preamble only, how will such a regime be coordinated with the entry into force of the multiple new national rules designed to apply the Regulation in each national state.

\* \* \*

# **CASE LAWS**

## I. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (IN NUMERICAL ORDER OF CASE NUMBER)

### 1. COURT OF JUSTICE DECISIONS

#### 1.1. C-450/00, COMMISSION V. LUXEMBOURG, 4.10.2001 ("LUXEMBOURG")

**Infringement procedure** against Luxembourg for failure to bring into force, within the prescribed period, the laws, regulations and administrative provisions necessary to comply with Directive 95/46/EC, as required under Article 32 of the Directive.

**Transposition:** Luxembourg argued that its delay in transposing the Directive was due to the new distribution of ministerial powers following a change in its internal government. The Court ruled that a Member State may not plead provisions, practices or circumstances in its internal legal system in order to justify a failure to comply with obligations and time limits laid down in a Directive, and thus a violation had occurred.

#### 1.2. C-465/00 AND C-138/01, RECHNUNGSHOF V. OSTERREICHISCHER RUNDFUNK, 20.5.2003 ("RECHNUNGSHOF")

**Reference for a preliminary ruling** by the Austrian Constitutional and Supreme courts. National legislation required public bodies subject to the control of the Rechnungshof (Court of Audit) to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners, together with the names of the recipients, for the purpose of it drawing up an annual report to be transmitted to the federal and provincial legislatures, and the general public. The defendants, subject to this requirement, refused, claiming that they are not obliged to communicate such data relating to income on grounds of data protection requirements.

**Questions referred:** (1) Whether data protection law precludes national legislation which requires a state body to collect and transmit data on income for the purpose of publishing the names and income of various state employees; (2) Whether provisions precluding such national legislation are directly applicable, in the sense that the persons obliged to disclose may rely on them to prevent the application of the national provisions.

**Scope of Directive 95/46:** Applicability of Directive 95/46 cannot depend on whether the specific situations at issue have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty (here free movement of workers). The EU system of data protection has a wide scope, is defined in very broad terms, and does not depend on whether, in every specific case, the processing of personal data has a connection to the free movement between the Member States. A contrary interpretation could make the limits of the field of application of the Directive unsure

and uncertain. The system consists of checks and balances in which processing of personal data is subject to a number of conditions and limitations.

**Article 8 ECHR:** Provisions of Directive 95/46, insofar as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in light of that right, which forms an integral part of the general principles of EU law. Article 8 ECHR states that public authorities must not interfere with the right to respect for private life, unless it is in accordance with law and is necessary in a democratic society to protect certain interests.

The collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8. The ECHR has held that communication of the data infringes the right of the persons concerned to respect for private life.

Regarding necessity, the purpose of the provision was to keep salaries within reasonable limits, which fits within the “economic well-being of the country”. But “necessary” means that a pressing social need is involved and the measure is proportionate to the legitimate aim pursued. The 6 authorities enjoy a margin of appreciation. The interests of the state must be balanced against the seriousness of the interference. The interference is justified only insofar as publication of the names is both necessary and appropriate to the aim of keeping salaries within reasonable limits, which is for the national court to examine. If not, then the interference also constitutes a violation of Articles 6 and 7 of Directive 95/46.

**Direct applicability:** Wherever provisions of a directive appear to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any incompatible national provision, or insofar as they define rights which individuals are able to assert against the State.

### 1.3. C-101/01, LINDQUIST, 6.11.2003 (“LINDQUIST”)

**Reference for a preliminary ruling** by the Swedish appellate court. Mrs. Lindquist had published on the internet the names, jobs, hobbies, telephone numbers, family circumstances etc. of 18 colleagues, as well as the fact that one had injured her foot and was on medical leave. She removed the data as soon as some objected. She was charged with criminal violations of Swedish data protection law.

**Questions referred:** (1) Whether the mention of a person, by name or with name and telephone number, on an internet home page is an action which falls within the scope of Directive 95/46; (2) If so, whether the loading of information of this type about work colleagues onto a private home page which is accessible to anyone who knows its address is covered by one of the exceptions under Article 3(2) of Directive 95/46; (3) Whether information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds is personal data concerning health which, according to Article 8(1), may not be processed; (4) Whether the

loading of the data onto the home page, with the result that the data becomes accessible to people in third countries, constitutes a transfer to a third country; (5) Whether a Member State can provide more extensive protection for personal data than the directive.

**Definition of personal data:** The name of a person in conjunction with his/her telephone number, and information about working conditions or hobbies constitute personal data. **Definition of processing:** The operation of loading personal data on an internet page must be considered to be processing.

**Scope of Directive 95/46:** Loading personal data on an internet page is processing by automatic means.

**Processing for purely personal or household activity:** Mrs. Lindquist's activities were mainly charitable and religious, but these are not covered by the exceptions in Article 3(2) of the Directive and cannot be considered exclusively personal or domestic.

**Sensitive personal data:** Reference to the fact that an individual has injured her foot and is on medical leave constitutes personal data concerning health within the meaning of Article 8(1), as that provision must be given a wide interpretation so as to include all aspects, both physical and mental, of the health of an individual.

**Transfers to third countries:** The publication on the internet did not constitute a transfer, as an internet user would have to connect to the internet and personally carry out the necessary actions to consult those pages. Mrs. Lindquist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access. There is no transfer of data to a third country within the meaning of Article 25 of the Directive when an individual in a Member State loads personal data onto an internet page which is stored with his/her hosting provider in that or another Member State, thereby making the data accessible to anyone who connects to the internet, including people in a third country.)

**Balancing fundamental rights:** The data protection and freedom of expression must be balanced against each other, and the regime of the Directive provides in itself multiple mechanisms allowing a balancing of the different fundamental rights to be carried out. Therefore, it is not a disproportionate violation of the principle of freedom of expression.

**Transposition/Harmonisation:** The Directive envisages complete harmonisation, thus Member States must adopt national legislation conforming to the regime of the Directive. However, certain provisions of the Directive can explicitly authorize the Member States to adopt more constraining regimes of protection. This must be done in accordance with the objective of maintaining a balance between free movement of personal data and protection of private life. In addition, Member States remain free to regulate areas excluded from the scope of application of the Directive in their own way, provided no other provision of EU law precludes it.

#### **1.4. C-317 AND 318/04, PARLIAMENT V. COUNCIL (PNR), 30.5.2006 (“PNR”)**

Action for annulment by the European Parliament of Council Decision 2004/496/EC concerning the conclusion of an agreement between the EU and the USA on the processing and transfer of Passenger Name Record (PNR) data and on the adequacy decision on data transferred to the USA, both of which were adopted on the basis of Directive 95/46. After the 11 September 2001 terrorist attacks, the US passed legislation providing that air carriers operating flights to or from the US or across the US had to provide US customs with electronic access to the data contained in their automated reservation and departure control systems (PNR). Negotiations followed, and in April 2004, the Commission adopted the decision on adequacy and the Council adopted the decision on conclusion of an agreement between the EU and the US on the processing and transfer of PNR data.

##### **Appropriate legal basis:**

- Adequacy decision: Requirements for transfer were based on a statute enacted by the USA in November 2001 and implementing Regulations adopted thereunder, which concern enhancement of security and conditions under which persons may enter and leave the USA, fighting against terrorism and fighting transnational crime. Thus, the transfer of PNR data is processing concerning public security.

Even though PNR data are initially collected in the course of commercial activity, the processing addressed in the adequacy decision concerns safeguarding public security and law enforcement. The facts that the data are collected by private operators for commercial purposes and that those operators arrange for the transfer of the data to the third country does not prevent that transfer from being regarded as processing excluded from the Directive's scope. Thus, it falls within the first indent of Article 3(2) of the Directive, which excludes from the Directive's scope data protection in the course of activities provided for by Titles V and VI of the EU Treaty. Accordingly, the adequacy decision is annulled.

- Agreement: Article 95 of the EC Treaty (internal market) in conjunction with Article 25 of the Directive (transfers to third countries ensuring adequacy) do not justify EU competence to conclude the Agreement. The agreement relates to the same transfers as the adequacy decision, and thus processing operations are outside the scope of the Directive. The Council decision approving the conclusion of the agreement between the EU and the US on the processing of PNR data is annulled.

#### **1.5. C-275/06, PROMUSICAE, 29.1.2008 (“PROMUSICAE”)**

**Reference for a preliminary ruling** by the Juzgado de lo Mercantil No. 5 de Madrid. Telefonica had refused to disclose to Promusicae, an NPO acting on behalf of its members who are holders of intellectual property rights, personal data relating to users of the internet who accessed the KaZaA file exchange program and shared files of recordings of Promusicae's members, by means of connections provided by Telefonica. Promusicae wanted to bring civil actions against those persons.

**Question referred:** Whether EU law permits Member States to limit the duty of operators of telecom networks to supply traffic data.

**Balancing fundamental rights:** The requirements of protection of different fundamental rights must be reconciled, namely the right to respect for private life on the one hand and rights to protection of property and an effective remedy on the other hand. Directive 2002/58 provides rules determining in what circumstances and to what extent personal data processing is lawful and what safeguards must be provided.

**Transposition/Harmonisation:** Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in civil proceedings, nor does it oblige them to impose such an obligation. However, when transposing various intellectual property Directives, Member States must take care to interpret them such that there is a fair balance struck between the various fundamental rights protected by the Community legal order. Further, when implementing the national law transposing those Directives, authorities and courts of the Member States must interpret them in a manner consistent with the Directives and make sure that the interpretation does not conflict with those fundamental rights or other general principles of Community law, such as the proportionality principle.

#### **1.6. C-301/06, IRELAND V. PARLIAMENT AND COUNCIL, 10.2.2009 ("IRELAND")**

**Action for annulment** by Ireland regarding Directive 2006/24/EC on the retention of electronic communication data on the ground that it was not adopted on an appropriate legal basis (Article 95 EC Treaty), amending Directive 2002/58 (also based on Article 95).

**Appropriate legal basis:** The Court rejected Ireland's argument that the sole or principal objective of the Directive is investigation, detection and prosecution of crime. Article 95(1) provides that the Council is to adopt measures for approximation of provisions laid down by law, regulation or administrative action in the Member States, which have the objective of establishment and functioning of the internal market. It may be used where disparities exist (or are likely to exist in the future) between national rules, which obstruct fundamental freedoms or create distortions of competition and thus have a direct effect on the functioning of the internal market. The premise of the Directive was to harmonize disparities between national provisions governing retention of data by service providers, particularly regarding the nature of data retained and periods of data retention. It was apparent that differences were liable to have a direct impact on the functioning of the internal market, which would become more serious with the passage of time.

Article 47 of the EU Treaty provides that none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty, in order to safeguard the building of the *acquis communautaire*. Insofar as Directive 2006/24 comes within the scope of

Community powers, it could not be based on a provision of the EU Treaty without infringing Article 47. Directive 2006/24 provisions are limited to activities of service providers and do not govern access to data or use thereof by police or judicial authorities of the Member States. They are designed to harmonize national laws on the obligation to retain data, the categories of data to be retained, the periods of retention of data, data protection and data security, and the conditions for data storage. They do not involve intervention by police or law enforcement authorities of Member States, nor access, use or exchange by them. Thus Directive 2006/24 relates predominantly to the functioning of the internal market.

### 1.7. C-524/06, HUBER V. GERMANY, 16.12.2008 (“HUBER”)

**Reference for a preliminary ruling** by the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Germany). Huber, an Austrian national resident in Germany, requested the deletion of personal data relating to him (name, date and place of birth, nationality, marital status, sex, entries and exits from Germany, residence status, particulars of passports, statements as to domicile, reference numbers) in the German Central Register of Foreign Nationals (AZR). The Bundesamt assists public authorities responsible for the application of the law related to foreign nationals and asylum. The AZR is used for statistical purposes and by security and police services and judicial authorities for the prosecution and investigation of criminal activities. Germany rejected Huber’s request.

**Question referred:** Whether the processing of personal data of an Austrian national in the AZR is compatible with the requirement of necessity under Article 7(e) of Directive 95/46.

**Scope of Directive 95/46:** Article 3(2) excludes from the scope of Directive 95/46 the processing of personal data concerning public security, defense, and criminal law activities. Thus, in this case, only processing for a purpose relating to the right of residence and for statistical purposes falls within the scope of Directive 95/46.

**Necessity:** In light of the fact that Directive 95/46 is intended to ensure an equivalent level of data protection in all Member States, to ensure a high level of protection in the EU, the concept of necessity in Article 7(e) cannot have a meaning which varies among Member States. Thus, it is a concept which has its own independent meaning in EU law, and must be interpreted in a manner which fully reflects the objective of Directive 95/46.)

Under EU law, the right of free movement of a Member State national is not unconditional, but may be subject to limitations and conditions imposed by the Treaty and implementing rules. Legislation provides that a Member State may require certain documents to be provided to determine the conditions of entitlement to the right of residence. Thus, it is necessary for a Member State to have relevant particulars and documents available to it in order to ascertain whether a right of residence in its territory exists. Use of a register to support authorities responsible for application of the legislation on the right of residence is, in principle, legitimate.



However, the register must not contain any information other than what is necessary for that purpose, and must be kept up to date. Only anonymous information is required for statistical purposes. Access must be restricted to the responsible authorities. The central register could be necessary if it contributes to a more effective application of that legislation. The national court should decide whether these conditions are satisfied.

### **1.8. C-73/07, TIETOSUOJAVALTUUTETTU [FINNISH DATA PROTECTION OMBUDSMAN] V. SATAKUNNAN MARKKINAPORSSI OY AND SATAMEDIA OY, 16.12.2008 (“TIETOSUOJAVALTUUTETTU”)**

**Reference for preliminary ruling** by the Korkein hallinto-oikeus (administrative court, Helsinki). Defendant 1: (a) collected public personal data (the name of persons whose income exceeded a threshold, the amount of earned and unearned income, and the wealth tax levied) from Finnish tax authorities and (b) published extracts in a regional newspaper each year. The newspaper stated that personal data can be removed on request without charge. Defendant 1 also: (c) transferred the data on CD ROM to Defendant 2 (owned by the same shareholders) which (d) disseminated them by text messaging system.

**Questions referred:** (1) | Whether collection, publication, transfer of a CD ROM and text messages constitutes processing of personal data; (2) Whether it is processing for solely journalistic purposes within the meaning of Article 9 of Directive 95/46; (3) Whether Article 17 and principles of Directive 95/46 preclude publication of data collected for journalistic purposes and their onward transfer for commercial purposes; (4) Whether personal data that have already been published in the media fall outside scope of Directive 95/46.

**Definition of personal data:** Surname, given name of certain natural persons whose income exceeds certain thresholds as well as the amount of their earned and unearned income constitute personal data.

**Definition of processing:** All four types of activities constitute processing of personal data. This includes personal data that have already been published in unaltered form in the media. Operations referred to in Article 2(b) must be classified as processing where they exclusively concern material that has already been published in unaltered form in the media. A general derogation from the application of the Directive in such a case would largely deprive the Directive of its effect.

**Scope of Directive 95/46:** Only two exceptions to scope exist, which are set forth in Article 3(2). The first indent states that security and criminal law are activities of the state. The second indent states that processing by a natural person in the course of a purely personal or household activity concerns activities in the course of private or family life of individuals. Activities (c) and (d) are activities of private companies, and are not within the scope of Article 3(2). A general derogation from application of the Directive in respect of published information would largely deprive the Directive of its effect. Thus activities (a) and (b) are also not within the scope of Article 3(2).

**Processing for solely journalistic purposes:** Article 1 of the Directive indicates that the objective is that Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to processing of their personal data. That objective can only be pursued by reconciling those fundamental rights with the fundamental right to freedom of expression. The objective of Article 9 is to reconcile the two rights. Member States are required to provide derogations in relation to protection of personal data, solely for journalistic purposes or artistic or literary expression, which fall within the fundamental right to freedom of expression, insofar as necessary for reconciliation of the two rights. To take account of the importance of the right of freedom of expression in every democratic society, it is necessary to interpret notions of freedom, such as journalism, broadly. Derogations must apply only insofar as strictly necessary. The fact that publication is done for profit making purposes does not preclude publication from being considered as "solely for journalistic purposes." The medium used is not determinative of whether it is "solely for journalistic purposes." Thus activities may be classified as "journalistic" if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them.

### **1.9. C-518/07, COMMISSION V. GERMANY, 9.3.2010 ("GERMANY")**

**Infringement procedure** against Germany, which transposed the second paragraph of Article 28(1) of Directive 95/46 (the requirement for an independent data protection Authority (DPA)) by making the authorities responsible for monitoring personal data processing outside the public sector in the different Lander subject to State oversight.

**Independence of DPA:** Independence normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. There is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. The adjective "complete" implies a decision-making power independent of any direct or indirect external influence on the supervisory authority. The guarantee of independence of DPAs is intended to ensure the effectiveness and reliability of the supervision of compliance with data protection provisions, to strengthen the protection of individuals and bodies affected by their decisions. DPAs must act impartially and must remain free from any external influence, including that of the State or Lander. Independence precludes not only any influence exercised by supervised bodies, but also any directions or other external influence which could call into question the performance of those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data. State scrutiny in principle allows the government of the respective Land to influence the decision of the supervisory authority or cancel and replace those decisions. This is not consistent with the principle of independence.

### 1.10. C-553/07, COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN ROTTERDAM V. RIJKEBOER, 7.5.2009 (“RIJKEBOER”)

**Reference for a preliminary ruling** by the Raad van State (Netherlands). Dutch law on personal data held by local authorities provides that on request, the Board of Aldermen must notify a data subject within four weeks whether his personal data have been disclosed to a purchaser or third party during the preceding year. Data held by the authority include basic data (name, date of birth, personal identification number, social security number, local authority of registration, etc.) and data on transfers. Mr. R requested to be informed of all instances where data relating to him were transferred in the preceding two years, and of the content and recipients. Dutch law on local authority personal records limited the communication of data to one year prior to the relevant request.

**Questions referred:** Whether the restriction provided for in the Netherlands law on local personal records on the communication of data to one year prior to the relevant request is compatible with Article 12(a) of Directive 95/46, whether read in conjunction with Article 6(1)(e) and the principle of proportionality.

**Right of access:** Right of access is necessary to enable the data subject to exercise his other rights (rectification, blocking, erasure, and notify recipients of same; object to processing or request damages). The right must of necessity relate to the past, otherwise the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for damages. Member States have some freedom of action in implementing the Directive, but it is not unlimited. Setting of a time limit on the right of access must allow the data subject to exercise his rights. It is for the Member States to fix a time limit for storage of information on the recipients and the content of the data disclosed, and to provide access to that information which constitutes a fair balance between the interest of the data subject in exercising his rights and the burden on the controller to store that information. In the present case, limiting storage of information on recipients and content to one year, while the basic data is stored much longer, does not constitute a fair balance, unless it can be shown that longer storage would constitute an excessive burden.

### 1.11. C-557/07, LSG-GESELLSCHAFT ZUR WAHRNEHMUNG VON LEISTUNGSSCHUTZRECHTEN GMBH V. TELE2 TELECOMMUNICATION GMBH, 19.2.2009 (“LSG”)

**Reference for a preliminary ruling** by the Oberster Gerichtshof (Austria). The applicant is a collecting society, which as trustee enforces rights of recorded music producers in their worldwide recordings and of the recording artists in exploitation of those recordings in Austria. Tele2 is an Internet Service Provider (ISP) that assigns an IP address to its clients. LSG applied to the Austrian court for an order requiring

Tele 2 to send names and addresses of persons to whom it had provided internet access service and whose IP addresses and date and time of connection were known.

**Question referred (partial listing):** Does Article 8(3) of Directive 2004/48, regard being had to Articles 6 and 15 of Directive 2002/58, not permit the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright?

**Balancing fundamental rights:** The judgment refers to 70 of the *Promusicae* judgment regarding balancing fundamental rights. That decision did not rule out the possibility that Member States may place an ISP under a duty of disclosure. An ISP provides a service which enables users to infringe copyright by providing a connection.

### **1.12. C-28/08, COMMISSION V. BAVARIAN LAGER CO., 29.6.2010 (“BAVARIAN LAGER”)**

**Appeal** by the Commission seeking annulment of the General Court judgment, which annulled the Commission's decision rejecting the request of the applicant (a trade association for German beer) for access to the full minutes of a meeting organized by the Commission (including names of attendees). The Commission had denied access to the names of five persons who attended the meeting, were members of a trade association and had not given consent to disclosure of their names, based on Article 4(1)(b) of Regulation 1049/2001. (The General Court decision, which was the subject of appeal, as well as the Advocate General's opinion, are summarized below.)

**Article 4(1)(b) exception:** The General Court erred in limiting application of the exception in Article 4(1)(b) to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the case law of the European Court of Human Rights, without taking into account the legislation of the EU concerning the protection of personal data, particularly Regulation 45/2001. It disregarded the wording of the Article, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the EU data protection legislation. The Article establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public.

Recital 15 of Regulation 45/2001 indicates legislative intent that Article 6 TEU and thereby Article 8 ECHR should apply where processing is carried out in the exercise of activities outside the scope of Regulation 45/2001 (Titles V and VI of pre-Lisbon TEU). Such reference was unnecessary for activities within the scope of Regulation 45/2001. Thus, where a request based on Regulation 1049/2001 seeks access to documents including personal data, Regulation 45/2001 becomes applicable in its entirety, including Articles 8 and 18. The General Court erred in dismissing the application of Article 8(b) and 18 of Regulation 45/2001, and its decision does not

correspond to the equilibrium, which the legislator intended to establish between the two Regulations. The Commission was right to verify whether the data subjects had given their consent to disclosure of personal data concerning them. By releasing the expurgated version of the minutes, with the names of five participants removed (three could not be contacted, two objected), the Commission did not infringe Regulation 1049/2001 and complied with its duty of openness. By requiring that regarding these five persons, the applicant establish the necessity for those personal data to be transferred, the Commission complied with the provisions of Article 8(b) of Regulation 45/2001. As no necessity was provided, the Commission was not able to weigh up the various interests of the parties concerned, nor to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by Article 8(b).

**Definition of personal data:** The General Court correctly held that surnames and forenames may be regarded as personal data. Thus, the list of names of participants in a meeting is personal data, since persons can be identified.

**Definition of processing:** Communication of personal data in response to a request for access to documents constitutes processing.

### **Opinion of Advocate General Sharpston, 15.10.2009**

**Scope of Regulation 45/2001:** Article 3(2) should be construed to define the circumstances in which the Regulation applies ("the processing of personal data wholly or partly by automatic means and . . . the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.") Such processing of personal data by all Community institutions is then covered (applying Article 3(1)) insofar as it is "carried out in the exercise of activities all or part of which fall within the scope of Community law"). Other circumstances are not covered by Regulation 45/2001; they should be dealt with under Regulation 1049/2001, where requests are made to Community institutions for access to documents.

**Article 4(1)(b) exception:** Applicability of Regulation 1049/2001 versus Regulation 45/2001 in request for access to documents: B-1 documents contain an incidental mention of personal data, where the primary purpose of compiling the document has little to do with personal data. The *raison d'être* of such documents is to store information in which personal data are of minimal importance. B-2 documents contain a large quantity of personal data (e.g. a list of persons and their characteristics). The *raison d'être* of such documents is to gather together such personal data.

- Applications for B-1 documents should be handled under Regulation 1049/2001, while applications for B-2 documents should be handled under Regulation 45/2001, because they are within its scope by virtue of Article 3(2).
- Requests for B-1 documents do not require a reason, by virtue of Article 6(1) of Regulation 49/2001, while requests for B-2 documents will have to demonstrate the need for transfer of data, in accordance with Article 8(b) of Regulation 45/2001.

- Article 8 ECHR (including the justification test, where interference with privacy exists) must be applied with respect to an application for B-1 documents to determine whether personal data must be redacted, following Article 4(1)(b) of Regulation 45/2001. B-2 documents will be subject to the procedure outlined in Regulation 45/2001: processing must be lawful within the meaning of Article 5. The applicant will have to give reasons in accordance with Article 8; Article 9 applies for applications from non-Member States or non-Community international organizations; Article 10 applies regarding sensitive data; and Article 18 requires the institution to inform the data subject that he can object to processing.
- Disclosure under Regulation 1049/2001 of B-1 documents is *erga omnes*; disclosure under Regulation 45/2001 of B-2 documents is case-by-case and not *erga omnes*.

The first part of the exception applies to B-1 and B-2 documents; the second part applies only to B-2 documents.

### **General Court decision, T-194/04, 8.11.2007**

**Lawfulness:** The right of access to documents of the institutions laid down by Article 2 of Regulation 1049/2001 constitutes a legal obligation for purposes of Article 5(b) of Regulation 45/2001. Therefore, if Regulation 1049/2001 requires communication of data, Article 5 of Regulation 45/2001 makes such communication lawful.

**Transfers:** Access to documents containing personal data falls within the application of Regulation 1049/2001. Article 6(1) states that the applicant is not required to justify his request. Therefore, where personal data are transferred in the context of Regulation 1049/2001, the applicant does not need to prove necessity of disclosure of data for purposes of Article 8 of Regulation 45/2001, otherwise it would be contrary to the principle of the widest possible public access to documents held by the institutions. Exceptions must be interpreted narrowly. Given that access to a document will be refused under Article 4(1)(b) of Regulation 1049/2001 where disclosure would undermine protection of privacy and integrity of the individual, a transfer that does not fall under that exception cannot, in principle, prejudice the legitimate interests of the person concerned within the meaning of Article 8(b) of Regulation 45/2001.

**Right to object:** The data subject has the right to object to processing, except in cases covered by Article 5(b), among others. Given that processing envisaged by Regulation 1049/2001 constitutes a legal obligation for purposes of Article 5(b), the data subject does not have a right to object. However, since Article 4(1)(b) of Regulation 1049/2001 lays down an exception to the obligation to provide access, it is necessary to consider the impact of disclosure on the data subject. If communication would not undermine protection of privacy etc., then the person's objection cannot prevent disclosure.

**Balancing fundamental rights:** Regulation 45/2001 must be interpreted in light of fundamental rights, which form an integral part of general principles of law with respect to which the ECJ ensures compliance.

**Article 8 ECHR:** ECHR case law interprets "private life" broadly, and there is no reason in principle to exclude professional or business activities from the concept of private life. To determine whether there is a breach of Article 8, it is necessary to determine (1) whether there has been an interference with private life of the data subject, (2) whether that interference is justified (i.e., it is in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society – meaning that it is relevant and sufficient, and proportionate to the legitimate aims pursued). In cases concerning disclosure of personal data, the competent authorities have to be granted a certain discretion in order to establish a fair balance between competing public and private interests, subject to judicial review, referring to factors such as nature and importance of interests at stake and seriousness of interference.

Any decision taken pursuant to Regulation 1049/2001 must comply with Article 8 ECHR.

**Article 4(1)(b) exception:** To determine whether the exception applies, it is necessary to examine whether public access is capable of actually and specifically undermining the protection of the privacy and integrity of the persons concerned.

The mere fact that a document contains personal data does not necessarily mean that privacy or integrity of the data subject is affected, even though professional activities are not, in principle, excluded from the concept of private life. Here, persons present at the meeting whose names were not disclosed were present as representatives of a trade association, and not in their personal capacity. Therefore, the fact that the minutes contain their names does not affect their private life. The minutes do not contain their personal opinions. Disclosure of the names is not capable of actually and specifically affecting the protection of privacy and the integrity of those persons. The mere presence of their name on the list does not constitute an interference. Regulation 45/2001 does not require the Commission to keep secret the names of persons who communicate opinions or information to it concerning the exercise of its functions.

The court distinguishes the *Osterreichischer Rundfunk* decision on the ground that there, the specific combination of name and income received was at issue, in contrast to this case, where the name of persons acting in a professional capacity as representatives of a collective body is at issue, where no personal opinions can be identified.

### **1.13. C-92/09 VOLKER UND MARKUS SCHECKE GBR V. LAND HESSEN, AND C-93/09, EIFERT V. LAND HESSEN AND BUNDESANSTALT FÜR LANDWIRTSCHAFT UND ERNÄHRUNG, 9.11.2010 ("SCHECKE")**

**Reference for a preliminary ruling** by the Verwaltungsgericht Wiesbaden (Germany). A partnership established in the Land of Hesse and a farmer resident there received EU funds from the EAGF and EAFRD. The defendant's website published the name and address of beneficiaries, plus annual amounts received, in accordance with Regulation 1290/2005 (rules on financing of expenditure falling

under CAP) and Regulation 259/2008 (requiring publication exclusively on the internet). The applicants filed an action in national court to prevent publication of data relating to them.

**Question referred:** Whether provisions requiring publication of this data on the Internet are valid and consistent with data protection requirements.

**Legal persons:** Legal persons can claim protection of Articles 7 and 8 of the CFR only insofar as the official title of the legal person identifies one or more natural persons. Here, the name of the legal person directly identifies the natural persons who are its partners.

**Consent:** The legislation at issue does not seek to base the personal data processing for which it provides on consent of the beneficiaries concerned. Rather, it provides that they are to be informed. Thus, processing is not based on their consent. Therefore, it is necessary to analyse whether interference is justified under Article 52(1) of the CFR.

**Articles 7/8 CFR:** The validity of legislation requiring publication must be assessed in light of provisions of the CFR, including Article 8. However, CFR Article 52(1) accepts that limitations may be imposed on rights under the CFR, as long as they are provided by law, respect the essence of those rights and are proportionate (necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.) Further, CFR Article 52(3) states that for rights in the CFR which correspond to rights in the ECHR, the meaning and scope shall be same as that given in the ECHR.

Publication on the website of data naming beneficiaries and amounts they receive constitutes interference with private life under Article 7 of the CFR. It is irrelevant that the data concerns activities of a professional nature, as under Article 8 ECHR, the CFR has held that no principle justifies exclusion of activities of a professional nature from the notion of private life.

Publication must a) be provided by law, b) respect the essence of the rights and freedoms in Articles 7 and 8 of the CFR, and c) be proportionate (necessary and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Here, publication is lawful since it is specifically provided for by the Regulation. It meets the general interest requirement because publication is intended to enhance transparency regarding use of CAP funds and sound financial management. Regarding proportionality, it is necessary to analyse whether the EU balanced its interest in guaranteeing transparency and ensuring the best use of public funds with the rights of beneficiaries to privacy and data protection. Derogations to data protection are allowed only insofar as they are strictly necessary.

- For natural persons, there is nothing to show that lawmakers made an effort to strike a balance. No automatic priority can be conferred on the objective of transparency over data protection, even if important economic interests are at stake. Thus, the lawmaker exceeded the limits, which the proportionality principle imposes.



- Publication of the data in question with respect to the complainant legal person does not go beyond limits imposed by the proportionality principle. The seriousness of the breach manifests itself in different ways for legal persons versus natural persons. It would impose an unreasonable administrative burden on the competent national authorities if they were obliged to examine, before the data are published for each legal person who is a beneficiary, whether the name of that person identifies natural persons. Thus, the legislation requiring publication is valid with respect to the legal persons.

#### **1.14. CASE C-70/10, SCARLET EXTENDED SA V. SOCIETE BELGE DES AUTEURS, COMPOSITEURS ET EDITEURS SCRL (SABAM), 24.11.2011 (“SCARLET”)**

**Reference for a preliminary ruling** by the cour d’appel de Bruxelles (Belgium). SABAM, a management company representing authors, composers and editors of musical works, brought proceedings in the Belgian court against Scarlet, an internet service provider (ISP), to take measures to bring an end to copyright infringements committed by Scarlet's customers. Scarlet had been ordered by the Belgian court of first instance to install a system for filtering electronic communications which use file-sharing software (“peer-to-peer”), with a view to preventing file sharing which infringes copyright. Scarlet appealed. The court of appeal referred the question for preliminary ruling.

**Question referred:** Whether EU Directives on electronic commerce in the internal market, intellectual property rights and data protection, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be construed as precluding an injunction on an ISP to introduce such a filtering system.

**Definition of personal data:** ISP addresses are protected personal data because they allow the concerned users to be precisely identified.

**Necessity/proportionality:** The contested filtering system may infringe the right to protection of personal data of the ISP's customers, as it would involve a systematic analysis of all content and the collection and identification of the users' IP address from which unlawful content on the network is sent.

**Balancing fundamental rights:** The injunction to install the contested filtering system did not respect the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information.

### 1.15. CASE C-461/10, BONNIER AUDIO AB ET AL. V. PERFECT COMMUNICATION SWEDEN, 19.4.2012 (“BONNIER”)

**Reference for a preliminary ruling** by the Högsta domstolen (Sweden). The applicants, which are publishing companies that hold copyrights to 27 audiobooks, brought proceedings in the Swedish court for copyright infringement by means of a file transfer protocol (FTP) server which allows file sharing and data transfer via the internet. The applicants applied to the Swedish court for an order for the disclosure of the name and address of the person using the IP address from which the files were sent. EPhone, the ISP, challenged the application, alleging that it violated the Data Retention Directive.

**Questions referred:** (1) Whether Directive 2006/24 precludes the application of a national provision which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which it is claimed was used in the infringement; (2) whether the answer to the first question is affected by the fact that the Member State has not implemented Directive 2006/24.

**Scope of Directive 2006/24:** Directive 2006/24 deals exclusively with the handling and retention of data generated by electronic communication service providers for the purpose of the investigation, detection, and prosecution of serious crime and their communication to competent national authorities. Thus, a national provision transposing the EU intellectual property directive, which permits an ISP in civil proceedings to be ordered to give a copyright holder information on the subscriber to whom the ISP provided an IP address allegedly used in an infringement, is outside the scope of Directive 2006/24 and therefore not precluded by that Directive. It is irrelevant that the Member State concerned has not yet transposed Directive 2006/24.

**Definition of processing:** Communication of the name and address sought by applicants constitutes processing of personal data.

**Scope of Directive 2002/58:** The communication of the name and address in question falls within the scope of Directive 2002/58 (and within the scope of Directive 2004/48, dealing with copyright).

**Balancing fundamental rights:** The national legislation in question requires, for an order for disclosure of the data in question to be made, that there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into a copyright infringement and that the reasons for the measure outweigh the potential harm to the person affected. Thus, it enables the national court seized of an application for an order for disclosure of personal data to weigh the conflicting interests involved, and thereby in principle ensures a fair balance between protection of intellectual property rights and protection of personal data.

### 1.16. JOINED CASES C-468/10 AND C-469/10, ASOCIACION NACIONAL DE ESTABLECIMIENTOS FINANCIEROS DE CREDITO (ASNEF) AND FEDERACION DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECMD) V. ADMINISTRACION DEL ESTADO, 24.11.2011 (“ASNEF”)

**Reference for a preliminary ruling** by the Tribunal Supremo of Spain. The applicants in national proceedings challenged the validity of Royal Decree 1720/2007 implementing Organic Law 15/1999. These national rules provide that, in the absence of the interested party's consent, and to allow processing of his personal data that is necessary to pursue a legitimate interest of the controller or recipients, it is necessary not only that the fundamental rights and freedoms of the data subject should not be prejudiced, but also that the data should appear in public sources. These requirements go beyond the provisions of Article 7(f) of Directive 95/46.

**Questions referred:** Whether a Member State can add new principles relating to the lawfulness of processing of personal data to those specified in Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7; Whether Article 7(f) has direct effect.

**Transposition/harmonisation:** Harmonisation of national laws is not limited to minimal harmonisation but harmonisation which is generally complete. Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of data subjects, equivalent in all Member States. Consequently, Article 7 of Directive 95/45 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as lawful. That interpretation is corroborated by the term “may be processed only if”, which demonstrates the exhaustive and restrictive nature of the list appearing in that Article. Thus, the Member States cannot add new principles relating to the lawfulness of processing or impose additional requirements.

Article 5 authorises Member States to specify the conditions under which the processing of personal data is lawful, within the limits of Article 7, *inter alia*. That margin of discretion can be used only in accordance with the objective pursued by the Directive of maintaining a balance between the free movement of personal data and the protection of private life. A distinction must be made between national measures that provide for additional requirements amending the scope of a principle referred to in Article 7 (precluded) and national measures which provide for a mere clarification of one of those principles (allowed). Thus, Article 7(f) precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in that Article.

**Balancing fundamental rights:** The second condition of Article 7(f) (the interests of the controller or recipients must not be overridden by the fundamental rights and freedoms of the data subject) necessitates a balancing of the opposing rights and

interests concerned, which depends on the individual circumstances of the particular case. In relation to the balancing, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources. The processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and recipients, which is a more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights, and must be properly taken into account in the balancing. However, it is no longer a precision within the meaning of Article 5 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing the result of the balancing thereby not allowing a different result by virtue of the particular circumstances of an individual case.

**Direct applicability:** Whenever the provisions of a Directive appear to be unconditional and sufficiently precise, they have direct effect if the Member State has failed to implement that Directive in domestic law by the end of the prescribed period. Article 7(f) is sufficiently precise, as it states an unconditional obligation.

### 1.17. C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 ("AUSTRIA")

**Infringement procedure** against Austria, alleging that it incorrectly transposed the second paragraph of Article 28(1) of Directive 95/46 (the requirement for an independent Data Protection Authority (DPA)), insofar as the national legislation does not allow the Data Protection Commission (DSK) to exercise its functions "with complete independence."

**Independence of DPA:** By failing to take all measures necessary to ensure that the Austrian national legislation meets the requirement of independence with regard to the DSK, Austria has failed to fulfill its obligations under the second subparagraph of Article 28(1) of Directive 95/46 and Article 8(3) of the EU Charter of Fundamental Rights and Article 16(2) TFEU. The establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data.

The words "with complete independence" must be given an autonomous interpretation. Supervisory authorities must enjoy an independence which allows them to perform their duties free from external influence, direct or indirect, which is liable to have an effect on their decisions. The fact that DSK has functional independence insofar as its members are "independent and [are not] bound by instructions of any kind in the performance of their duties" is an essential, but not sufficient, condition to protect it from all external influence. Here, the national legislation provides only for the operational autonomy of the supervisory authority, but does not preclude the DSK from performing its duties free from all indirect influence, for the following reasons:

(1) The managing member of the DSK need not always be an official of the Federal Chancellery (although it always has been), and all day-to-day business is thus *de facto* managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision. It is conceivable that the evaluation of the managing member by his hierarchical superior for the purposes of encouraging his promotion could lead to a form of “prior compliance”. Moreover, the Chancellery is subject to the supervision of the DSK, so the DSK is not above all suspicion of partiality. The service-related link between the managing member of the DSK and the Chancellery affects the DSK's independence. The fact that the appointment of the managing member rests on an autonomous decision of the DSK does not protect the independence of the supervisory authority;

(2) The office of the DSK is structurally integrated with the departments of the Federal Chancellery, and all DSK staff are under the authority of the Federal Chancellery and subject to its supervision. The DSK need not be given a separate budget to satisfy the criterion of independence. They can provide that the DPA comes under a specified ministerial department. However, the attribution of the necessary equipment and staff to DPAs must not prevent them from acting with complete independence. Here, since they are subject to supervision by the Chancellery, it is not compatible with the requirement of independence.

(3) The Federal Chancellor has the right to be informed of all aspects of the work of the DSK. This precludes the DSK from operating above all suspicion of partiality.

### 1.18. C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 (“AUSTRIA”)

**Reference for a preliminary ruling** by the Bundesgerichtshof, Germany. The applicant (Probst) is the recipient of internet services supplied by Verizon through, and billed by, Deutsche Telecom. The respondent (mr.nexnet) is the assignee of claims for payment for the supply of internet services by Verizon. The applicant failed to pay some of the charges. The contract between legal predecessors of the respondent and Verizon provided that personal data would be processed exclusively for the purpose of that contract, and deleted immediately thereafter.

**Questions referred:** Whether Directive 2002/58 permits the passing of traffic data from the service provider to the assignee of a claim for payment in respect of telecommunications services in the case where the assignment effected with a view to the collection of transferred debts includes, in addition to the general obligation to respect the privacy of telecommunications and to ensure data protection as provided for under the applicable legislation, contractual stipulations that: (1) the service provider and assignee undertake to process the personal data only within the framework of their cooperation and exclusively for the purpose of the contract; (2) as soon as the data is no longer required for such purpose, the data will be erased or returned; (3) each contracting party is entitled to check that the other has ensured data protection and security in accordance with the agreement; (4) confidential documents and information transferred may be made accessible only to such

employees as required for purposes of performing the contract; (5) those employees are required to maintain confidentiality; (6) on request or termination of the cooperation between the contracting parties, the data will be erased or returned.

**Traffic data:** Article 6(2) of Directive 2002/58 provides an exception to the confidentiality of communications, stating that traffic data necessary for purposes of subscriber billing and interconnection payments may be processed “up to the end of the period during which the bill may lawfully be challenged or payment pursued.” Thus, the provision covers the processing necessary for securing payment, including debt collection. Article 6(5) provides that traffic data processing authorized by Article 6(2) “must be restricted to persons acting *under the authority of* [the service] providers of the public communications networks and publicly available electronic communications services handling billing” and “must be restricted to what is necessary” for the purpose of such activity. Thus, the assignee of claims for payment is authorized to process the data on condition that it acts “under the authority” of the service provider and that it processes only traffic data which are necessary for the purpose of recovery of those claims. That provision seeks to ensure that such externalization of debt collection does not affect the level of protection of personal data enjoyed by the user. “Under the authority” must be strictly construed to mean that the assignee acts only on instructions and under the control of the service provider. The contract between the service provider and assignee must contain provisions ensuring the lawful processing of traffic data by the assignee and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee.

### **1.19. C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 (“GOOGLE”)**

**Reference for a preliminary ruling** by the Audiencia Nacional (Spain). Mr. G, a Spanish national resident in Spain, sued Google Spain, Google Inc. and La Vanguardia newspaper, alleging that when an internet user entered his name in the Google search engine, he would obtain links to two pages of La Vanguardia newspaper on which an announcement with his name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts. He requested *inter alia* that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. The DPA granted the request against Google Spain and Google Inc. Information indexed by Google Search following the location and sweeping of websites throughout the world by its web crawlers is stored temporarily on servers whose state of location is unknown. Google provides results with advertising associated with the user’s search terms. The subsidiary Google Spain promotes the sale of advertising in Spain, and was registered as the controller of related processing in Spain.

**Questions referred:** (1) Whether an “establishment” exists where one or more of the following circumstances arises: the undertaking providing the search engine sets up in a Member State an office or subsidiary to promote and sell advertising space on the search engine, or when the parent designates a subsidiary in that Member State as its representative and controller for two specific filing systems which relates to the data of customers who have contracted for advertising, or when the office or subsidiary forwards to the parent, located outside the EU, requests and requirements addressed to it both by data subjects and DPAs; (2) Whether there is a “use of equipment ...situated on the territory of the said Member State” under Article 4(1)(c) of Directive 95/46 when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State or when it uses a domain name pertaining to a Member State and arranges for searches and the results to be based on the language of that Member State; (3) Whether the temporary storage of the information indexed by internet search engines is a “use of equipment” under Article 4(1)(c); (4) Whether Directive 95/46 must be applied, in light of Article 8 of the CFR, in the Member State where the centre of gravity of the conflict is located; (5) Does the activity of Google Search fall within the concept of processing in Article 2(b) of Directive 95/46; (6) Whether the undertaking managing Google Search is a controller of the personal data contained in the web pages that it indexes; (7) Whether the DPA can directly impose on Google Search a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located; (8) Whether the obligation of search engines to protect those rights would be excluded when the personal data has been lawfully published by third parties and is kept on the web page from which it originates; (9) Whether the rights of erasure, blocking and objection of Directive 95/46 extend to enabling the data subject to address himself to search engines in order to prevent indexing of the data, published on the third parties’ web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though it has been lawfully published by third parties.

**Definition of processing:** The operation of loading personal data on an Internet page must be considered processing (as the court held in *Lindquist*). In exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine “collects” such data which it subsequently “retrieves”, “records” and “organizes” within the framework of its indexing programmes, “stores” on its servers and, as the case may be, “discloses” and “makes available” to its users in the form of lists of search results, which constitute processing, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. This finding is not affected by the fact that those data have already been published on the Internet and are not altered by the search engine. It is not necessary that the personal data be

altered. While alteration of personal data constitutes processing under Article 2(b), the other operations mentioned there do not require the alteration of personal data.

The processing done by the search engine operator is distinguished from and in addition to that done by publishers of websites, consisting in loading those data on an Internet page.

**Definition of controller:** The search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity and is thus a controller. It would be contrary not only to the clear wording of Article 2(d) and to its objective, which is to ensure through a broad definition of the concept of controller, effective and complete protection of data subjects, to exclude the operator of a search engine on the ground that it does not exercise control over the personal data published on the web pages of third parties. Moreover, the activity of search engines plays a decisive role in the overall dissemination of the personal data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published. The search results also provide a structured overview of the information relating to that individual that can be found on the Internet, enabling them to establish a detailed profile of the data subject. The fact that publishers of websites have the option of indicating to operators by means of exclusion protocols that they wish some information published on their site to be excluded from the search engines' automatic indexing does not mean that if publishers do not so indicate, the operator of the search engine is released from responsibility for its processing of personal data.

### **Scope of Directive 95/46:**

- Google Spain is an “establishment” within the meaning of Article 4(1)(a). It engages in the effective and real exercise of activity through stable arrangements in Spain, and is a subsidiary of Google Inc. on Spanish territory.
- The processing of personal data by the controller is also “carried out in the context of the activities” of an establishment, even though Google Spain is not involved in the processing at issue (which is carried out exclusively by Google Inc.) but rather only in advertising in Spain. Article 4(1)(a) does not require that the processing in question be carried out “by” the establishment concerned, but only “in the context of the activities” of the establishment. In light of the objective of effective protection of fundamental rights, those words cannot be interpreted restrictively. The activities of the search engine and those of its establishment in the Member State are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine economically profitable and that engine is the means enabling those activities to be performed.

**Data subject rights:** The non-compliant nature of processing may arise from the breach of any conditions of lawfulness imposed by the Directive, including data quality and legitimacy. Here, the grounds for legitimacy were those specified in



Article 7(f), which permits processing where necessary for the purposes of the legitimate interests pursued by the controller or third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights of the data subject. This requires a balancing of interests. Balancing provided in Article 14 allows account to be taken of all circumstances surrounding the data subject's particular situation.

- **Interest of the data subject:** The search of the individual's name enables any internet user to obtain, through a list of results, a structured overview of the information relating to that data subject that can be found on the internet. This may potentially concern a vast number of aspects of his private life enabling a detailed profile. Without the search engine, this data could not have been interconnected or only with great difficulty. The interference with the rights of the data subject is heightened because of the important role played by the Internet and search engines in modern society.
- **The interests of the search engine:** These are economic interest, which cannot justify the potential seriousness of the interference with the data subject's rights.
- **Interests of the internet users:** The data subjects' rights generally override those of internet users, but the balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, which may vary by the role played by the data subject in public life. The interference may be justified by the preponderant interests of the general public in having access to the information.
- **The Supervisory authority or judicial authority** may order the search engine operator to remove the link from the list of results without presupposing the previous or simultaneous removal of the underlying information from the web page on which it was published. Requiring the data subject to obtain erasure from web pages would not provide effective and complete protection of data subject, especially because publishers may not be subject to EU data protection law or publication may be carried out "solely for journalistic purposes" and thus benefit from derogation. Further, balancing would be different for processing by the search engine and processing by the web publisher.

**Right of erasure:** The search engine operator must erase information and links concerned in the list of results if that information appears, having regard to all circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine. Here, having regard to the sensitivity for data subject's private life of information contained in announcements and the fact that the initial publication occurred 16 years earlier, the data subject has established that the links should be removed.

## 1.20. C-141/12 AND C-372/12, MINISTER VOOR IMMIGRATIE V. M, 17.7.2014 (“M”)

**Reference for a preliminary ruling** by the Rechtbank Middelburg and the Raad van State. Several third country nationals applied for a residence permit for a fixed period in the Netherlands. One applicant asked for a residence permit for a fixed period, which was denied, the other asked for the same, which was granted. Both asked for a copy of the minute, which explained the decision, and both were denied access.

**Questions referred (partial listing):** (1) Whether the second indent of Article 12(a) of Directive 95/46 should be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, or is it sufficient if a full summary, in an intelligible form, of such data is provided; (2) Whether the words “right of access” in Article 8(2) CFR should be interpreted to mean there is a right to a copy of documents; (3) Whether a legal analysis, as set out in a “minute”, can be regarded as personal data; (4) Whether protection of the rights and freedoms of others under Article 13(1)(g) of Directive 95/46 can cover the interest in an internal undisturbed exchange of views within the public authority concerned.

**Definition of personal data:** The data relating to the applicant for a residence permit included in the minute (applicant’s name, DOB, nationality, gender, ethnicity, religion and language) constitute personal data. The legal analysis in the minute may contain personal data but it does not in itself constitute such data. The legal analysis is not information relating to the applicant, but at most, in so far as not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant’s situation. This interpretation is consistent with the language of Article 2(a) and the objective and general scheme of Directive 95/46.

**Right of access:** Regarding the right of access, protection of the fundamental right to respect for private life means that the data subject may be certain that the personal data concerning him are correct and that they are processed lawfully. It is in order to carry out the necessary checks that the data subject has, under Article 12(a), a right of access, which is necessary to obtain rectification, erasure or blocking of his data (Article 12(b)). The legal analysis is not in itself liable to be the subject of a check of its accuracy by the applicant and rectification, while the facts are. Moreover, the right of access is not designed to ensure the greatest possible transparency of the decision-making process of public authorities and to promote good administrative practices (as is the case for the right of access to documents).

To comply with the right of access under Article 12(a) and Article 8(2) of CFR, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with the Directive. He need not be given a copy of the documents.

### 1.21. C-288/12, COMMISSION V. HUNGARY, 8.4.2014 (“HUNGARY”)

**Infringement procedure** against Hungary for failure to fulfil obligations under Article 258 TFEU. Mr. J was appointed for 6 years as DPA. However, pursuant to transitional measures related to revision of data protection law, Hungary prematurely ended his term and appointed a new DPA for 9 years.

**Independence of DPA:** Establishment in a Member State of an independent supervisory authority is an essential component of the protection of individuals with regard to the processing of personal data. Operational independence of supervisory authorities, in that members are not bound by instructions of any kind in the performance of their duties, is an essential condition that must be met to respect the independence requirement, but this is not sufficient.

The mere risk that the state could exercise political influence over decisions of a supervisory authority is enough to hinder independence. If it were permissible for the Member State to compel the supervisory authority to vacate office before serving his/her full term, even if this comes about as a result of restructuring or changing of the institutional model, the threat of such premature termination could lead the supervisory authority to enter into a form of prior compliance with the political authority. This is incompatible with the requirement of independence, and the supervisory cannot be regarded as being able to operate above all suspicion of partiality. Member States are free to adopt or amend the institutional model they consider most appropriate for supervisory authorities. However, they must ensure that the independence of the authority is not compromised, which entails the obligation to allow that authority to serve his/her full term.

### 1.22. C-291/12, SCHWARZ V. BOCHUM, 17.10.2014 (“SCHWARZ”)

**Reference for a preliminary ruling** by the Verwaltungsgericht Gelsenkirchen (Germany). Applicant applied to Stadt Bochum for a passport, but refused to have his fingerprints taken, and Stadt therefore refused his application. He brought an action before the referring court to have a passport issued without taking his fingerprints.

**Questions referred (partial listing):** Is Article 1(2) of Regulation 2252/2004 to be considered valid, on the ground that it breaches certain fundamental rights of the holders of passports issued in accordance with that provision.

**Definition of personal data:** Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows them to be identified with precision.

**Definition of processing:** Taking and storing fingerprints constitute processing.

**Articles 7 and 8 CFR:** Taking and storing of fingerprints by national authorities, governed by Article 1(2) of Regulation 2252/2004, constitute a threat to the rights of respect for private life and protection of personal data.

Article 52(1) allows for limitations on exercise of rights in Articles 7 and 8 CFR as long as limitations are provided for by law, respect the essence of those rights, and respect proportionality (necessary and genuinely meet objectives of general interest recognised by EU or need to protect rights and freedoms of others). Here, taking of fingerprints for passports is provided by Regulation 2252/2004 to prevent falsification of passports and fraudulent use thereof, and illegal entry into the EU. Therefore, the provision pursues an objective of general interest recognised by the EU.

**Consent:** It is essential for citizens of the EU to own a passport in order to travel to a third country, and a passport must contain fingerprints. Therefore, citizens are not free to object to processing of their fingerprints, and thus persons applying for passports cannot be deemed to have consented to that processing.

**Necessity/proportionality:** Storage of fingerprints on a highly secure storage medium is likely to reduce risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders, although it is not wholly reliable. Thus, it is appropriate.

The action involves taking prints of two fingers, causing no physical or mental discomfort, plus a facial image. The only real alternative to fingerprints is iris scan, the technology of which is not yet as advanced as fingerprint recognition. Thus, there is no apparent alternative that is sufficiently effective and less of a threat to the protected rights.

The concern that data may be centrally stored and used for other purposes (e.g. criminal investigation or monitor the person indirectly) does not affect the validity of the Regulation, which provides only for preventing illegal entry into EU.

### **1.23. C-293/12 AND C-594-12, DIGITAL RIGHTS IRELAND LTD V. IRELAND, 8.4.2014 (“DRI”)**

**Reference for a preliminary ruling** from the High Court (Ireland) and the Verfassungsgerichtshof (Austria). Digital Rights Ireland brought an action in High Court claiming that it owned a mobile phone which it used since 2006, challenging national measures requiring retention of data relating to electronic communications and asking the court to declare the invalidity of Directive 2006/24, which requires telephone communications service providers to retain traffic and location data for a period specified by national law to prevent, detect, investigate and prosecute crime and safeguard security.. This data that which is necessary to trace and identify the source of a communication and its destination, the date, time, duration and type of a communication, users’ communication equipment, and location of mobile equipment including name and address of subscriber, calling telephone number, number called and IP address for internet users.

The directive does not permit the retention of content, but it might have an effect on the use of the means of communication and consequently on the exercise of freedom

of expression guaranteed by Article 11 CFR. It also directly affects private life (guaranteed by Article 7 CFR) and constitutes processing of personal data (therefore falls under Article 8 CFR).

**Articles 7 and 8 CFR:** The obligation on providers of publicly available electronic communications services or public communications networks to retain data relating to a person's private life and his communications in itself constitutes an interference with Article 7. Access of competent national authorities to the data constitutes a further interference with that right. The Directive constitutes an interference with Article 8 because it provides for processing of personal data. These interferences with Articles 7 and 8 are wide-ranging and particularly serious. The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of users the feeling that their private lives are the subject of constant surveillance.

Any limitation on the exercise of rights and freedoms laid down by CFR must be provided by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. Even though retention constitutes a particularly serious interference with the right to privacy, it is not such as to adversely affect the essence of those rights given that the Directive does not permit the acquisition of knowledge of the content of the electronic communications. Nor does it adversely affect the essence of the right to protection of personal data because certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or public communications networks, in order to ensure appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

**Directive 2006/24:** The material objective of the Directive is of general interest – to ensure that data are available for the purpose of the investigation, detection and prosecution of serious crime, and therefore to public security, and international terrorism. (Article 6 CFR lays down the right of any person to liberty and security.) Data relating to use of electronic communications are particularly important and a valuable tool in prevention of offences and the fight against crime.

**Necessity/proportionality:** The principle of proportionality requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation and do not exceed the limits of what is appropriate and necessary to achieve those objectives. Here, given the important role played by data protection in light of the fundamental right of privacy, and the extent and seriousness of the interference, the EU legislature's discretion is reduced, thus the review of that discretion should be strict. Retention of data is an appropriate tool for the objective pursued.

The fight against serious crime and terrorism is of the utmost importance to ensure public security and its effectiveness may depend on the use of modern investigation techniques. But this does not, in itself, justify the necessity of the retention measure. Derogations and limitations in relation to data protection must apply only insofar as strictly necessary. Here, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees effectively to protect their personal data against the risk of abuse, and unlawful access and use of the data. The need for safeguards is all the greater where personal data are subjected to automatic processing and there is significant risk of unlawful access to the data. Further, the Directive requires retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony – i.e. all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. This covers all subscribers and registered users, and therefore entails an interference with the fundamental rights of practically the entire European population, without a need for a link to crime.

**Lawfulness:** The Directive fails to lay down objective criteria by which to determine the limits of access of competent national authorities to the data and its use, nor substantive and procedural conditions relating to access by competent national authorities and to their subsequent use. It does not lay down objective criteria to limit the number of persons authorized to have access and use to what is strictly necessary, and it is not made dependent on prior review carried out by a court or independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of obtaining the objective pursued.

**Retention:** The Directive establishes a retention period of a minimum of 6 months and a maximum of 24 months, but it is not stated that determination of this period must be based on objective criteria to ensure that it is limited to what is strictly necessary

**Security:** The Directive does not provide for sufficient safeguards to ensure effective protection of the data retained against risk of abuse and unlawful access. It does not lay down rules adapted to the vast quantity of data whose retention is required, the sensitive nature of that data, and the risk of unlawful access, nor is there a specific obligation set on Member States to establish such rules. Rather, it permits providers to have regard to economic considerations when determining the level of security.

**Supervision:** The Directive does not require that the data be retained within the EU, with the result that it cannot be held that the control by an independent authority of compliance with the requirements of data protection and security is fully guaranteed. This is an essential component of protection of individuals with regard to the processing of personal data.)

**Necessity/proportionality:** Accordingly, the EU legislature exceeded limits imposed by compliance with principle of proportionality in light of Articles 7, 8 and 52(1) CFR.

#### **1.24. C-342-12, WORTEN-EQUIPAMENTOS PARA O LAR SA V. ACT (AUTHORITY FOR WORKING CONDITIONS), 30.5.2013 (“WORTEN”)**

**Reference for a preliminary ruling** from Tribunal do Trabalho de Viseu (Portugal). Worten (a private company in Portugal) adopted a system of restricted access to working hour records of staff, which did not allow ACT to have automatic access. ACT considered this a serious offence of national law on workers and imposed a fine.

**Questions submitted:** (1) Whether the record of working time for each worker is covered by the concept of personal data under Article 2 of Directive 95/46; (2) If so, whether the Portuguese state is obliged to provide appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network; (3) When the Member State does not adopt any such measure, and the employer as controller does not allow automatic access by the national authority responsible for monitoring working conditions, whether the principle of the primacy of European law is to be interpreted to mean that the Member State cannot penalize the employer for that action?

**Personal data definition:** Data contained in a record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent “information relating to an identified or identifiable natural person.

**Security:** Article 17(1) requires controllers (not Member States) to adopt technical and organizational measures which, having regard to the state of the art and cost of their implementation, are to ensure a level of security appropriate to the risks represented. The obligation under national law to provide the national authority responsible for monitoring working conditions with immediate access to the record of working time does not imply the data must be made accessible to persons not authorised for that purpose (as Worten claimed). Rather, Worten must ensure that only those persons duly authorised to access the personal data in question are entitled to respond to a request for access from a third party. Thus, Article 17(1) is not relevant here.

**Necessity/proportionality:** The referring court must verify that the personal data contained in the record of working time are collected in order to ensure compliance with the national legislation relating to working conditions, that the processing of those data is necessary for compliance with a legal obligation to which Worten is subject and the performance of the monitoring task entrusted to the national authority responsible for monitoring working conditions. Only the grant of access to authorities having powers of monitoring could be considered to be necessary within

the meaning of Article 7(e). Further, the obligation to provide immediate access to the record could be necessary if it contributes to the more effective application of the legislation relating to working conditions. It is for referring court to decide whether this requirement is necessary.

Proportionality: Penalties must respect the principle of proportionality.

### 1.25. C-473/12, IPI V. ENGLEBERT (“ENGLEBERT”)

**Reference for a preliminary ruling** by the Belgian constitutional court. The applicant is responsible for ensuring compliance with conditions of access to and proper practice of the profession of estate agent. It asked the Charleroi commercial court to declare that defendants had violated applicable rules and should cease various estate agency activities, based on facts gathered by private detectives. The question arose whether the private detectives had acted in breach of national data protection provisions, because they had not informed defendants before collecting their data (Article 10 of Directive 95/46), or third parties at the time of collection of the data (Article 11 of Directive 95/46).

**Questions referred:** (1) Whether Article 13(1)(g) leaves the Member States free to choose whether to provide for an exception to the immediate obligation to inform set out in Article 11(1) if this is necessary in order to protect the rights and freedoms of others, or are the Member States subject to restrictions in this matter; (2) Whether the professional activities of private detectives, governed by national law and exercised in the service of authorities authorized to report to judicial authorities any infringement of the provisions protecting a professional title and organizing a profession, comes within the exception in Article 13(1)(d) and (g); (3) Whether that Article is compatible with Article 6(3) TEU, the principle of equality and non-discrimination.

**Definition of personal data:** Data collected by private detectives relating to persons acting as estate agents concern identified or identifiable natural persons, and therefore constitute personal data.

**Transposition/harmonisation:** Article 13(1) states “Member States may” and thus does not oblige the Member States to lay down in their national law exceptions for the purposes listed therein. Rather, they have the freedom to decide whether, and for what purposes, to take legislative measures aimed at limiting the extent of the obligations to inform the data subject. Further, they may take such measures only when necessary.

**Derogations:** The activity of a body such as IPI (a professional body responsible for ensuring compliance with the rules governing the profession of estate agent which is a regulated profession in Belgium, through investigating and reporting breaches of those rules) corresponds to “the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions” and is capable of coming under that exception. The directive does not prevent such a professional



body from having recourse to private investigators. Thus, if a Member State has chosen to implement the exception, then the professional body and private detectives may rely on it and are not subject to the obligation to inform the data subject. However, if the Member State has not implemented the exception, the data subjects must be informed.

Rules on access to a regulated profession form part of the rules of professional ethics, therefore investigations concerning the acts of persons who breach those rules by passing themselves off as estate agents are covered by the exception in Article 13(1)(d).

### **1.26. C-486/12, X, 12.12.2013 (“X”)**

**Reference for a preliminary ruling** by the Gerechtshof te ‘s-Hertogenbosch (Netherlands). X requested her municipality to disclose her various addresses in 2008 and 2009 to prove that she had not received notices requesting payment of a fine for a traffic violation. The municipality responded with a certified transcript, demanding payment of a fee of EUR 12,80.

**Questions referred:** (1) Whether the provision of access to data pursuant to a provision under national law constitutes compliance with the obligation to communicate data undergoing processing (Article 12(a) of Directive 95/46); (2) Whether Article 12(a) precludes the levying of fees in respect of the communication, by means of a transcript from the municipal database, of personal data undergoing processing; (3) Whether the levying of the present fee is excessive.

**Access:** Article 12(a) of Directive 95/46 does not require Member States to levy fees when the right of access to personal data is exercised, nor does it prohibit the levying of such fees as long as they are not excessive. Access must be without constraint, without excessive delay and without excessive expense. The fees should be fixed at a level which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular his right to have the data communicated to him in an intelligible form, and on the other, the burden which the obligation to communicate such data represents for the controller. The fees may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access, and it should not exceed the cost of communicating such data.

### **1.27. C-212/13, RYNES V. ÚŘAD PRO OCHRANU OSOBNICH ÚDAJŮ, 11.12.2014 (“RYNES”)**

**Reference for a preliminary ruling** by the Nejvyšší správní soud (Czech Republic). The applicant (a private individual) installed and used a video camera system located under the eaves of his home, which recorded the entrance to his home, the public footpath and the entrance to the house opposite. The purpose was to protect the property, health and life of his family and himself, as they had been subjected to attacks by persons unknown whom it had not been possible to identify. A further

attack took place, which was recorded, and the recording made it possible to identify two suspects. The applicant provided the recording to the police who relied on it in subsequent criminal proceedings.

**Question referred:** Whether the operation of a camera system installed on a family home for the purposes of the protection of the property, health and life of the owners of the home can be classified as the processing of personal data “by a natural person in the course of a purely personal or household activity” for the purposes of Article 3(2) of Directive 95/46, even though such a system also monitors public space.

**Definition of personal data:** The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned.

**Definition of processing:** Video surveillance involving the recording and storage of personal data falls within the scope of the Directive, since it constitutes automatic data processing.

**Processing for purely personal or household activity:** Protection of the fundamental right to private life guaranteed under Article 7 of the CFR requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Also, the wording of the derogation refers to “purely” personal or household activity, not simply a personal or household activity. Correspondence and the keeping of address books constitute, in the light of recital 12 to Directive 95/46, a purely personal or household activity, even if they incidentally concern the private life of other persons. However, to the extent that the video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data, it cannot be regarded as a purely personal or household activity. Thus, the consent of the data subject would be required to process his data.

**Definition of controller:** Arts. 7(f), 11(2) and 13(1)(d) and (g) make it possible to take into account the legitimate interests of the controller in protecting the property, health and life of his family and himself.

## **1.28. C-615/13 P, CLIENT EARTH ET AL. V. EFSA, 16.7.2015 (“CLIENT EARTH”)**

**Appeal** from a judgment of the General Court dismissing an action for annulment of a decision of EFSA concerning access to documents. EFSA had developed a draft guidance on how to implement a provision of the Regulation of the European Parliament and of the Council concerning the placing of plant protection products on the market, which provided that “scientific peer-reviewed open literature, as determined by [the agency], concerning the side effects on health, the environment, and non-target species, shall be added by the applicant [for authorisation to place a plant protection product on the market].” A working group of the agency submitted the draft guidance to two EFSA bodies, some of whose members were external

experts, who were invited to submit comments on the draft guidance. As a result of the comments, the working group incorporated changes into the draft guidance. The guidance, as modified, was submitted for public consultation. EFSA stated that it redacted the names of the experts pursuant to Article 4(1)(b), because disclosure of the experts' names would be a transfer of personal data pursuant to Article 8, and the conditions for such transfer were not satisfied. The names of the experts concerned, together with the opinions expressed by them on the draft guidance, were published on the EFSA website.

The applicant requested access to several documents. EFSA granted partial access, but denied access in response to both the initial and confirmatory application to working versions of the draft guidance and comments of the experts on the draft. In a subsequent decision, EFSA granted the individual comments of the external experts, but redacted the names of the experts, pursuant to Article 4(1)(b) and Regulation 45/2001. It stated that provision of the names would constitute a transfer of personal data under Article 8 of Regulation 45/2001, and that the conditions for such a transfer were not fulfilled.

**Definition of personal data:** The information as to which expert is the author of each comment made by the external experts constitutes information, which falls within the scope of personal data. The fact that the information is provided as part of a professional activity does not mean that it cannot be characterized as personal data. The concepts of personal data and data relating to private life are not to be confused. The claim that the information concerned does not fall within the scope of private life is therefore ineffective.

Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance were made public on the EFSA website does not mean such data cannot be characterized as personal data. Finally, characterization of information relating to a person as personal data does not depend on whether the person objects to the disclosure of that information.

**Access:** Where an application is made seeking access to personal data, the provisions of Regulation 45/2001 (particularly Article 8(b)) become applicable in their entirety. Under Article 8(b), personal data may generally be transferred only if the recipient establishes necessity and if there is no reason to assume that the transfer might prejudice the legitimate interests of the data subject. Thus, the transfer is subject to these two cumulative conditions being satisfied. The applicant must establish the first condition, and the institution must determine whether there is such reason. If there is no such reason, the transfer must be made; if there is such reason, the institution must weigh the various competing interests in order to decide on the request.

**Necessity/proportionality:** No automatic priority can be conferred on the objective of transparency over the right to protection of personal data. However, the information was necessary to ensure the transparency of the process of adoption of a measure likely to have an impact on the activities of economic operators, in

particular, to appreciate how the form of participation by each expert might have influenced the content of that measure. Transparency of the process followed by a public authority for adoption of a measure contributes to the authority acquiring greater legitimacy in the eyes of the persons to whom the measure is addressed and increasing their confidence in that authority, and ensuring the authority is more accountable to citizens in a democratic system. Obtaining the information at issue was therefore necessary so that the impartiality of each expert in carrying out their tasks as scientists in the service of EFSA could be ascertained. Thus, the public interest justified the disclosure of the information at issue, in accordance with Article 8(a) and (b).

**Access to documents:** The consideration that disclosure was likely to undermine the privacy and integrity of the experts concerned is a consideration of a general nature not otherwise supported by any factor specific to the case. Disclosure would have made it possible for suspicions of partiality to be dispelled or allowed the experts to dispute the merits of those allegations. If a general consideration, unsupported by evidence, were to be accepted, it could be applied to any situation where an EU authority obtains experts opinions, contrary to the requirement that exceptions to the right of access to documents must be interpreted strictly. Thus, the conditions required by Article 8(b) were satisfied.

### **1.29. C-201/14, SMARANDA BARA ET AL. V. PRESEDINTELE CASEI NATIONALE DE ASIGURARI DE SANATATE (CNAS) ET AL., 1.10.2015 (“BARA”)**

**Reference for a preliminary ruling** by the Romanian Court of Appeal. Applicants earn income from self-employment. Data relating to their declared income was transferred by ANAF (the national tax authority) to CNAS (the national health insurance authority); the latter sought payment of arrears of contributions to the health insurance regime, based on this data. The applicants challenged the lawfulness of the transfer of tax data relating to their income, alleging that the data were used for purposes other than those for which they had initially been provided to ANAF, without their prior explicit consent and without having been previously informed.

**Questions referred (partial listing):** Whether personal data may be processed by authorities for which such data were not intended where such an operation gives rise, retroactively, to financial loss.

**Definition of personal data:** Tax data transferred are personal data, since they are “information relating to an identified or identifiable natural person.”

**Definition of processing:** Both the transfer of the data by ANAF, and the subsequent processing by CNAS, constitute processing of personal data.

**Information:** The requirement of fair processing laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of their data to another public administrative body for the purpose of their

processing by the latter in its capacity as recipient of those data. National law required the transfer of data necessary to certify that the person concerned qualifies as an insured person to CNAS. However, these do not include data relating to income, since the law recognises the right of persons without a taxable income as qualifying as insured. Thus, the national law cannot constitute “prior information” under Article 10 of Directive 95/46 (information requirement where data collected from the data subject), enabling the controller to dispense with his obligation to inform the data subject of the recipients of the income data, and the transfer therefore violated Article 10.

Article 11 (information requirement where data not collected from the data subject) requires that specified information be provided to the data subject, including the categories of data concerned and the existence of the rights of access and rectification. Thus, the data subjects should have been informed of the processing by CNAS and categories of data concerned, but CNAS did not so inform them. The Protocol between the two agencies does not establish rules for derogating from this requirement, either under Article 11 or 13 of the Directive.

**Derogations:** Article 13(1)(e) and (f) provide exceptions for important economic or financial interest of a Member State and monitoring, inspection or regulatory function, respectively. However, Article 13 expressly requires that such restrictions are imposed by legislative measures. Here, however, the transfer was made on the basis of a protocol between the two authorities, which is not a legislative measure, and is not subject to an official publication. Thus, the conditions of Article 13 were not complied with.

### **1.30. C-230/14, WELTIMMO S.R.O. V. NEMZETI ADATVEDELMI ES INFORMACIOSZABADSAG HATOSAG (HUNGARIAN DPA), 1.10.15 (“WELTIMMO”)**

**Reference for a preliminary ruling** by the Kuria (Hungary). The applicant, a Slovakian company with no registered office or branch in Hungary (but which carries out no activity where it has its registered office, in Slovakia), runs a website in Hungarian concerning Hungarian properties, with respect to which it processes the personal data of the advertisers. The advertisements are free of charge for one month but thereafter a fee is payable. Many advertisers sent a request by e-mail for deletion of their advertisements and their personal data following the one month period. The applicant did not delete the data and charged the interested parties for its services. These amounts were not paid, so the applicant forwarded the personal data of the advertisers to debt collection agencies. The advertisers lodged a complaint with the Hungarian DPA, which decided that the collection of the data constituted processing, and imposed a fine on the applicant for infringement of the Hungarian data protection law.

**Questions referred:** (1) Whether Article 28(1) of Directive 95/46 can be interpreted as meaning that the provisions of national law of a Member State are applicable in

its territory to a situation where the controller runs a property dealing website established only in another Member State and advertises properties in the territory of the first Member State and the property owners have forwarded their personal data to a facility for storage and data processing belonging to the operator of the website in that other Member State; (2) Whether Article 4(1)(a) (and other provisions) of Directive 95/46 can be interpreted as meaning that the Hungarian DPA may not apply Hungarian data protection law to an operator of a property dealing website established only in another Member State, even though it advertises Hungarian property whose owners transfer the data relating to such property probably from Hungarian territory to a server and processing belonging to the operator of the website; (3) Whether it is significant that the service provided by the controller of the website is directed at the territory of another Member State; (4) Whether it is significant that the data relating to the properties in the other Member State and the personal data of the owners are uploaded from the territory of the other Member State; (5) Whether it is significant that the personal data relating to those properties are that of citizens of another Member State; (6) Whether it is significant that the owners of the undertaking established in Slovakia live in Hungary; (7) Whether the Hungarian DPA can only exercise the powers provided by Article 28(3) of Directive 95/46 in accordance with the provisions of the national law of the establishment and accordingly not impose a fine.

**Definition of processing:** The operation of loading personal data on an internet page constitutes processing.

**Establishment of the controller:** Article 4(1)(a) of Directive 95/46 permits application of data protection law of a Member State other than the Member State in which the controller is registered, insofar as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity, even minimal, in the context of which the processing is carried out. To establish whether the controller has an establishment in that Member State, both the degree of stability of the arrangements and the effective exercise of activities in the other Member State must be interpreted in light of the specific nature of the economic activities and provision of services concerned, particularly for undertakings offering services exclusively over the internet. The presence of only one representative can suffice to constitute a stable arrangement if he/she acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State. Further, the concept of “establishment” extends to any real and effective activity, even a minimal one, exercised through stable arrangements.

Here, the activity of the controller consists in the running of property dealing websites concerning properties in Hungary and written in Hungarian and thus pursues a real and effective activity in Hungary. Further, it has a representative in Hungary responsible for recovering the debts resulting from that activity and representing the controller in administrative and judicial proceedings relating to the processing of the data concerned. It has a bank account in Hungary intended for the

recovery of debts and uses a letter box in Hungary for the management of everyday affairs. That is capable of establishing the existence of an “establishment”.

The processing is done in the context of the activities, which Weltimmo pursues in Hungary. Thus Hungarian data protection law would apply with respect to that processing. (By contrast the nationality of the persons concerned by such data processing is irrelevant.)

**DPA powers:** In the event that the Hungarian DPA should consider that Weltimmo has an establishment not in Hungary, but in another Member State, then in accordance with Article 28(4), it may exercise its powers conferred under Article 28(3) only within its own territory, and it may, irrespective of the applicable law and before even knowing which national law is applicable, thereby investigate the complaint. If it becomes apparent that it is the law of another Member State that applies, that DPA cannot impose penalties outside the territory of its own Member State. In fulfillment of the duty of cooperation laid down in Article 28(6), it requests the DPA of that Member State to establish an infringement of its national law and impose penalties if that law permits, based on the information which the first DPA has transmitted to second DPA. The second DPA may also find it necessary to carry out other investigations, on the instructions of the first DPA.

### 1.31. C-362/14, SCHREMS V. DATA PROTECTION COMMISSIONER, 6.10.2015 (“SCHREMS”)

**Reference for a preliminary ruling** by the Irish High Court. The applicant, an Austrian national residing in Austria, was a user of Facebook since 2008, for which he had concluded a contract with Facebook Ireland, a subsidiary of Facebook Inc. located in the USA. Some or all of Facebook Ireland’s users data of users who reside in the EU is transferred to the servers in the USA of Facebook Inc. and further processed. The applicant asked the defendant to prohibit Facebook Ireland from transferring his personal data to the USA, which does not ensure adequate protection against the surveillance activities engaged in there by public authorities, in particular the NSA. Defendant rejected the complaint on grounds that there was no evidence that it had been accessed by the NSA and that the Commission decision 2000/520 had found that the USA ensures an adequate level of protection in the Safe Harbor program.

**Questions referred:** (1) In the course of determining a complaint made to a national DPA that personal data is being transferred to a third country (the USA) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, whether that office holder is bound by the EU finding to the contrary in Decision 2000/520, having regard to Articles 7, 8 and 47 CFR, and the provisions of Article 25(6) of Directive 95/46 notwithstanding; (2) Whether the DPA may and/or must conduct his/her own investigation of the matter in the light of factual developments in the meantime since that Commission decision was first published.

**Independence of DPA:** The Directive seeks to ensure an effective, complete, and high level of protection of the fundamental rights and freedoms of natural persons. The guarantee of a DPA's independence is intended to ensure effectiveness and reliability of the monitoring of compliance, and is an essential component of data protection. DPAs powers extend to their own Member State, but not to processing in third countries. However, DPAs are responsible for monitoring transfers from a Member State to a third country, as the transfer is processing carried out in the Member State.

An adequacy decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46 is addressed to the Member States, which must take the necessary measures to comply with it. Until the Commission decision is declared invalid by the ECJ, it has legal effect in the Member States. However, it cannot eliminate or reduce the powers of the DPA accorded by Article 8(3) of the CFR, and therefore cannot prevent data subjects whose personal data has been transferred from lodging a claim pursuant to Article 28(4) with the DPA, alleging that an adequate level of protection is not ensured in that third country, which in essence challenges the validity of the Commission's adequacy decision. But the ECJ alone has jurisdiction to declare that the decision is invalid; neither the DPA nor a national court may do so. The latter must refer the claim to the ECJ for a preliminary ruling to examine the validity of the Commission decision.

Article 3 of Decision 2000/520 lays down specific rules regarding DPA's powers in light of a Commission adequacy finding (to suspend data flows to self-certified US organisations under restrictive conditions establishing a high threshold for intervention). It excludes the possibility of DPA's taking action to ensure compliance with Article 25 (adequacy), in particular, it denies DPAs powers which they derive from Article 28 to consider a data subject claim which puts into question whether a Commission adequacy decision is compatible with protection of privacy and fundamental rights and freedoms of individuals. This goes beyond the power conferred on the Commission in Article 25(6). Thus, Article 3 is invalid.

**Adequate level of protection:** The word "adequate" in Article 25(6) signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed by the EU legal order. However, it requires the third country to ensure, by reason of its domestic law or international commitments, a level of protection of fundamental rights and freedoms *essentially equivalent* to that guaranteed by the EU by virtue of Directive 95/46 read in light of the CFR, otherwise that protection could be easily circumvented by transfers. Thus, the legal order of the third country covered by a Commission adequacy decision must have means to ensure protection essentially equivalent to that guaranteed within the EU. When examining the level of protection afforded by a third country, the Commission must assess the content of the applicable rules resulting from domestic law or international commitments and the practice designed to ensure compliance. Also, in light of the fact that the level of protection ensured by the third country is liable to change, the Commission must, after adopting an adequacy decision, check periodically whether the adequacy



finding remains factually and legally justified. Account must be taken of the circumstances that have arisen after the adoption of the decision. The Commission's discretion as to adequacy is reduced and is subject to strict scrutiny, in view of the important role played by data protection in the light of the fundamental right to respect for private life and the large number of persons potentially concerned by transfers.

**Safe harbour:** US public authorities are not required to comply with safe harbor principles. Decision 2000/520 specifies that safe harbor principles may be limited to the extent necessary to meet national security, public interest or law enforcement requirements, or statute, regulation or case law. Self-certified US organisations receiving personal data from the EU are thus bound to disregard safe harbor principles when they conflict with US legal requirements. Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments.

**Interference with fundamental right:** Decision 2000/520 enables interference with the fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US.

**Necessity/proportionality:** The Decision does not contain any finding regarding US rules intended to limit the interference when they pursue legitimate objectives such as national security, nor refer to effective legal protection against such interference. FTC procedures and private dispute resolution mechanisms concern compliance with safe harbor principles (against US organisations) and cannot be applied with respect to measures originating from the State. Moreover, the Commission found that US authorities could access the personal data transferred and process it in a way incompatible with the purposes for which it was transferred, and beyond what was strictly necessary and proportionate for the protection of national security, and data subjects had no redress regarding their rights of access, rectification and erasure. Legislation permitting public authorities to have generalized access to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access, rectification or erasure of his own personal data does not respect the essence of the fundamental right to effective judicial protection.

Thus, Article 1 of the Decision does not ensure adequacy and the decision is consequently invalid.

Articles 1 and 3 are inseparable from 2 and 4 and the annexes, thus the entire Decision 2000/520 is invalid.

## 2. GENERAL COURT DECISIONS

### 2.1. T-320/02, ESCH-LEONHARDT AND OTHERS V EUROPEAN CENTRAL BANK, 18.2.2004 ("ESCH-LEONHARDT")

**Application for annulment** of ECB decision to include in applicants' personal files a letter concerning their use of the internal e-mail system for transmitting union information, and for damages.

**Definition of processing:** Inclusion of the letters in the personal files constitutes processing by saving data in a personal data filing system as provided in Article 2(a), (b) and (c) of Regulation 45/2001.

**Necessity/proportionality:** The ECB may be entitled to consider that inclusion of the letters is necessary for the performance of their contracts of employment. Insofar as the letters send a warning to those concerned, they relate to their administrative status and may become relevant for a report on their conduct in the service; thus it is appropriate to include them. A shortened version, omitting reference to relations between those concerned and the trade union, would not be sufficient for proper management of personal files. The fact that the staff in question contravened rules on the use of the ECB's internal email system by using it, as members of trade union, for purposes of that union, and not for gainful purposes, is liable to influence the assessment of their conduct in the service.

**Sensitive data:** Inclusion of the letters does not infringe Article 10(1) as it concerns data, which the persons themselves have manifestly made public within the meaning of Article 10(2)(d).

## **2.2. T-198/03, BANK AUSTRIA CREDITANSTALT AG V COMMISSION OF THE EUROPEAN COMMUNITIES, 30.5.2006 (“BANK AUSTRIA”)**

**Application for annulment** of decision of Commission's hearing officer to publish the non-confidential version of a Commission decision in a cartel case. The applicant (a legal person) argued, inter alia, that in numerous passages of the decision, it was possible to identify natural persons who participated on its behalf in meetings, the purpose of which was to restrict competition, which contravenes Regulation 45/2001.

**Legal person:** A legal person does not belong to the circle of persons which Regulation 45/2001 is intended to protect. That conclusion cannot be invalidated by the applicant's arguments of its supposed obligations towards directors and employees under Member State law, given that they consist of unsubstantiated contentions. These arguments are not sufficient to demonstrate the applicant's personal interest in relying on a breach of Regulation 45/2001.

## **2.3. T-259/03, NIKOLAOU V. COMMISSION, 12.9.2007 (“NIKOLAOU”)**

**Action for non-contractual liability** based on acts and omissions of OLAF. OLAF had disclosed certain information about its investigation concerning the applicant: a leak of information to a journalist; its annual report with information about the investigation; and its press statement. The applicant had requested access to the file and the final case report.

**Non-contractual liability:** Normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The Court concluded that the OLAF staff member leaked information (including PD) to a journalist, which was published, and OLAF's press release confirmed the veracity of facts (including PD) that had been mentioned in several press articles.

**Definition of personal data:** The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity.

**Definition of processing:** 1. the leak (unauthorised transmission of personal data to a journalist by someone inside OLAF) and

2. the publication of press release each constitute processing of personal data.

**Lawfulness:** The leak constitutes unlawful processing in violation of Article 5 of Regulation 45/2001 because it was not authorized by the data subject, not necessary under the other sub-paragraphs and it did not result from a decision by OLAF. Even though OLAF has a margin of discretion on transmissions, here it was not exercised because the leak is an unauthorized transmission. OLAF is best placed to prove how the leak occurred and that the Director of OLAF did not violate his obligations under Article 8(3) of Regulation 1073/99. In the absence of such proof, OLAF (the Commission) must be held responsible. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality.

Publication of the press release was not lawful under Article 5(a) and (b) because the public did not need to know the information published in the press release at the time of its publication, before the competent authorities had decided whether to undertake judicial, disciplinary or financial follow-up.

**Damages:** A violation of Regulation 45/2001 qualifies as an illegal act of an institution conferring rights on an individual. The objective of the Regulation is to confer such rights on DSs.

- A leak of personal data is necessarily a grave and manifest violation. The Director has a margin of appreciation on prevention, but here no showing was made regarding the exercise of the margin.
- OLAF gravely and manifestly exceeded the limits of its discretion in the application of Article 5(a) and (e), which was sufficient to engage the responsibility of the Community.
- 3000 euros damages were awarded.

## 2.4. T-161/04, JORDANA V. COMMISSION, 7.7.2011 (“JORDANA”)

**Action for annulment** of Commission decision refusing the applicant's request under Regulation 1049/2001 for access to the reserve list of successful candidates for a competition, in which he was himself a successful candidate, and for individual decisions nominating officials of grade A6 from 5.10.1995. The Commission had declined his request, based on the exception in Article 4(1)(b) of Regulation 1049/2001 regarding the right of privacy and integrity of the individual. The Commission reasoned that the candidates had not been informed in the notice of competition that the list of laureates would be published, and thus it would violate their private life to provide him with the list. The Commission stated in its reply that it may be possible for the applicant to gain access on the basis of Regulation 45/2001, and invited the applicant to present a request under that Regulation to the controller. The applicant's confirmatory application was also rejected. (The EDPS intervened in the case).

**Article 4(1)(b):** This provision is indivisible, and requires that the violation of private life and the integrity of the individual are always analyzed in conformity with the right to protection of personal data. Thus it establishes a specific regime where personal data may be communicated to the public. Since this case concerns the processing of personal data, the request must be analyzed under Regulation 45/2001. In rejecting the application for access to documents, the Commission had failed to apply Regulation 45/2001 in its analysis, and thus erred.

**Definition of personal data:** The first and last names of the persons on the reserve list and the officials mentioned in the individual decisions of appointment to grade A6 can be considered to fall within the personal data definition.

**Definition of processing:** Transfer of the data constitutes processing.

## 2.5. T-82/09, DENNEKAMP V. EUROPEAN PARLIAMENT, 23.11.2011 (“DENNEKAMP I”)

**Application for annulment** of European Parliament decision refusing to grant access to documents under Regulation 1049/2001 relating to the affiliation of certain MEPs to the additional pension scheme. Parliament had refused access on the ground that disclosure would be incompatible with Regulation 45/2001. At the hearing, the applicant submitted that he needed to have access to the personal data on grounds of public interest in accountability, transparency and control over public expenditure.

**Balancing fundamental rights:** Regulation 1049/2001 and Regulation 45/2001 do not contain any provisions granting one primacy over the other, therefore full application of both should, in principle, be ensured.

**Article 8(b):** Where a request based on Regulation 1049/2001 seeks access to documents containing personal data, Regulation 45/2001 becomes applicable in its

entirety, including Article 8. The applicant cannot claim that the processing he requested was lawful on the basis of Article 5(b) and this suffices, since Article 8(b) applies without prejudice to Article 5.

In order to obtain disclosure of the personal data contained in the documents, the applicant would have had to demonstrate, by providing express and legitimate justifications, the necessity for the requested personal data to be transferred, so that the Parliament could weigh up the various interests of the parties concerned and determine whether legitimate interests of MEPs might be prejudiced by the transfer. The applicant failed to establish why he needed the names to obtain his objectives. He did not explain with express arguments and justifications in what respect the transfer of the data was necessary to satisfy the public interest which he invoked, nor that the transfer would have been proportionate to his aims.

Further, the Parliament was not required to weigh the interests invoked by the applicant against those of MEPs, or to determine whether there was any reason to assume that the legitimate interests of those MEPs might have been prejudiced by such transfer. Thus, no manifest error that the Parliament might have made in weighing up interests has any bearing in this case on the lawfulness of the decision.

**Article 4(1)(b):** This is an indivisible provision requiring the institution concerned always to examine and assess any undermining of privacy and the integrity of the individual in conformity with Regulation 45/2001.

## **2.6. T-190/10, EGAN & HACKETT V. EUROPEAN PARLAMENT, 28.3.2012 (“EGAN & HACKETT”)**

**Application for annulment** of European Parliament decision denying access to certain documents. The applicants, who had worked for former MEPs, requested access to certain documents, which they stated they needed to commence legal proceedings. Among the documents requested were lists of assistants open for public inspection since 1984. Access was denied to the list on grounds of Article 4(1)(b) of Regulation 1049/2001 and Regulation 45/2001, except that lists open to the public during the period of professional activity of the persons.

**Scope of Regulation 45/2001:** Neither Article 2(3) of Regulation 1049/2001, nor Article 3(2) of Regulation 45/2001, nor any other provision, contains any restriction such as to exclude from their respective scopes documents, which were, but are no longer, available.

**Access:** The Parliament systematically took the view that the public should not have access to documents revealing the identity of former MEP assistants. It did not carry out an examination to show that the access would specifically and effectively undermine their privacy within the meaning of the provisions in question, nor did it verify whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. Thus, it failed to show to what extent disclosure would specifically and effectively undermine the right to privacy.

**Sensitive data:** The argument that release of names of former MEP assistants would reveal their political opinions and therefore constitute sensitive data was not substantiated and cannot make up for the fact that the contested decision failed to show why disclosure would specifically and effectively undermine their right to privacy within the meaning of Article 4(1)(b) of Regulation 45/2001.

## **2.7. T-115/13, DENNEKAMP V. EUROPEAN PARLIAMENT (15.7.2015) (“DENNEKAMP II”)**

**Application for annulment** of European Parliament decision refusing to grant access to documents under Regulation 1049/2001 relating to the affiliation of certain MEPs to the additional pension scheme. This case is related to case T-82/09, Dennekamp v. European Parliament, 23.11.2011. After receiving the judgment in that case, the applicant submitted a new request for access to four categories of documents relating to affiliation of certain MEPs to the additional pension scheme. He stated in the application that there was an objective necessity for the personal data to be transferred, relying on a broad public interest in transparency and how decisions were taken; that it was of the utmost importance for European citizens to know which MEPs had a personal interest in the additional pension scheme which involved the use of considerable public funds; and in the confirmatory application, he relied on the rights to information and freedom of expression. The EP denied access to three of the four categories, and confirmed the decision in response to the applicant’s confirmatory application. The applicant sought annulment of the EP’s decision.

**Transfers:** Articles 7-9 of Regulation 45/2001 precisely limit the possibility of transferring personal data so as to make it subject to strict conditions which, if not fulfilled, prohibit any transfer. Those conditions always include the necessity of the transfer in the light of various aims.

**Balancing fundamental rights:** If the applicant has established necessity, and the institution decides there is no reason to assume that DS’ legitimate interests may be prejudiced, the data may be transferred and the documents are to be made available to the public. To fulfill the condition of necessity under that article, an applicant for access to documents containing personal data must establish that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant’s objective, and it is proportionate to that objective, which means the applicant must submit express and legitimate reasons to that effect. This strict interpretation cannot be regarded as creating a broad exception to the fundamental right of access to documents, which would result in an unlawful restriction of that right. Rather, it reconciles two fundamental yet opposing rights, the institution being required also to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer. The general nature of the justification for transfer has no direct effect on whether the transfer is necessary for the purposes of attaining the applicant’s aim.

Here the applicant made two arguments to establish necessity. First, that necessity was based on the right to information and freedom of expression. These are not sufficient to establish that the transfer is the most appropriate of the possible measures for attaining the objective, or that it is proportionate to that objective. Moreover, the applicant did not make clear in what respect transferring the names of the MEPs participating in the scheme was the most appropriate measure for attaining the objective he had set for himself. He merely asserted that the measures designed to provide public control over public expenditure in the context of the additional pension scheme, like the discharge procedure, did not protect the fundamental right to information and to communicate it to the public. From this it cannot be determined in what respect the transfer would be the most appropriate measure, or how it is proportionate.

Second, the applicant argued that the transfer of personal data is necessary to determine whether MEPs' voting behavior regarding the additional pension scheme is influenced by their financial interest, and disclosure of all the names of the MEPs participating in the scheme would be the only way for the public to hold its representatives accountable for their actions in relation to the scheme. The court agreed that the transfer is the only measure by which the applicant's aim can be attained; no other measure is capable of ensuring that MEPs facing a potential conflict of interest are identified. Further, it is proportionate for this purpose.

The EU institution or body in receipt of the application must refuse the transfer if there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced. MEPs as public figures have chosen to expose themselves to scrutiny by third parties, particularly the media and general public, even if such choice in no way implies that their legitimate interests must be regarded as never being prejudiced by a decision to transfer their data. Thus, they have generally already accepted that some of their personal data will be disclosed to the public. That must be taken into account when assessing the risk of prejudice to their legitimate interests. Particular consideration should be given to the link between the personal data at issue and their mandate, and to the legal and financial commitment of the EP to the scheme. In view of the importance of the interests invoked here, which are intended to ensure the proper functioning of the EU by increasing the confidence that citizens may legitimately place in the institutions, the legitimate interests of the MEPs who are members of the scheme cannot be prejudiced by the transfer of personal data at issue.

An institution, which refuses access on the ground of prejudice to legitimate interests must state reasons for invoking such interests. The institution must explain how disclosure of a document could specifically and actually undermine the interest protected by the exception. The explanation cannot consist of a mere assertion that access would undermine privacy. Examination of the specific and actual nature of the undermining of the interest under Article 4(1)(b) of Regulation 1049/2001 is in dissociable from the assessment of the risk that the legitimate interests of the data subject referred to in Article 8(b) of Regulation 45/2001 which,

through the disclosure to the public, might be prejudiced by the transfer of personal data.

## **2.8. T-496/13, MCCULLOUGH V. CEDEFOP (11.6.2015)(“MCCULLOUGH”)**

**Application for annulment** of Cedefop’s decision refusing access to documents. The applicant, who had been employed by Cedefop, requested access to the minutes of all meetings of various internal groups for a specified period stating that he needed them to prepare his defence in legal proceedings between him and Cedefop pending before the Greek courts. Access was denied on the basis of Article 4(1)(b) and 4(3), and on grounds that Cedefop was not in possession of some of the requested documents, in response to the initial and confirmatory applications. Regarding minutes of the Governing Board and its Bureau, Cedefop considered that the names of the members which were contained in those minutes constituted personal data protected by Regulation 45/2001, and access could lead to a serious violation of the privacy and integrity of the members, as their opinions would be clearly shown in the documents. The applicant argued that the names and functions of the members of Cedefop’s Governing Board and Bureau are not personal data and that Cedefop’s statement that disclosure of the members’ opinions and views would violate their privacy is contrary to the principle of transparency (among others).

**Definition of personal data:** Surnames are personal data and therefore are protected by Regulation 45/2001. The fact that the members of Cedefop’s decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, and that the surnames were published in the OJ or on the internet, does not affect the characterization of the surnames as personal data.

**Transfer:** Applicant cannot be deemed to have proved the necessity of having the personal data at issue transferred. The only justification provided was to supplement his written defence before the Greek Examining Magistrate. Applicant did not provide any information or justification as to how the submission of the requested documents containing that data would affect the Greek proceedings, the risks to which he would be exposed in procedural terms, and the merits of his defence if the documents were not submitted to the Greek Magistrate.

**Article 4(1)(b):** Exceptions under Article 4 must be interpreted and applied strictly. An institution refusing access must explain how disclosure of that document could specifically and actually undermine the interest protected by the exception. The fact that a document concerns an interest protected by an exception is not of itself sufficient to justify application of that exception. Rather, it is necessary for the institution to have previously determined (1) that the document would specifically and actually undermine the protected interest and (2) that the risk of the protected interest being undermined is reasonably foreseeable and not purely hypothetical. The institution must explain how granting access to the document could specifically and actually undermine the interest protected by the exception under Article 4(1)(b).



Here, Cedefop simply states that the persons concerned are protected as individuals and any access would lead to a serious violation of the privacy and integrity of the individual as they clearly demonstrated the opinions and views of the members on the subject matters discussed. However, Cedefop neither carried out an examination demonstrating that granting access to those documents would specifically and actually undermine the privacy of those members within the meaning of Article 4(1)(b), nor verified whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. It is not apparent how the opinions and views expressed could fall within the sphere of their privacy, since those meetings were professional.

### 3. CIVIL SERVICE TRIBUNAL DECISIONS

#### 3.1. F-30/08, NANOPOULOS V. COMMISSION, 11.5.2010 (“NANOPOULOS”) (ON APPEAL, CASE T-308/10)

**Action for non-contractual liability** against the Commission pursuant to Article 340 TFEU. A journalist sent a letter to the Commission asking about anonymous allegations that the applicant favored companies of his own nationality in performing his duties as a Director in the Commission. The Commission reassigned the applicant to a post of principal advisor to the Director General, and opened a disciplinary proceeding against the applicant. Two leaks occurred: one concerning the plan to reassign the applicant; and one concerning the Commission's decision to open a disciplinary proceeding against the applicant. Journal Articles thereafter were published with the applicant's name including these facts.

**Non-contractual liability:** The normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The publication of the applicant's name could only have resulted from a leak by the Commission. The burden of proof was on the Commission to prove that it was not the source of the leak.

**Damages:** The leak by the Commission of the complainant's name as one of the officials undergoing a disciplinary procedure constitutes a violation of Regulation 45/2001, which was sufficient to engage its responsibility. 90.000 euros damages were awarded (70.000 moral prejudice and 20.000 fault of service linked to moral prejudice).

#### 3.2. F-46/09, V & EDPS V. EUROPEAN PARLAMENT, 5.7.2011 (“V”)

**Application for annulment** of a decision of the European Parliament, withdrawing a 2008 offer of employment to the applicant on grounds of unfitness to be hired. The

Commission Medical Service had determined that the applicant was not fit; she had appealed, and the Commission had affirmed the conclusion. She filed an Article 90 complaint, which the Commission rejected, then a lawsuit against that decision, which the Court of First Instance rejected. In 2008, she was offered a post as contractual agent with the Parliament. The Parliament requested and received a copy of her medical file from the Commission medical service and thereafter withdrew its offer on the ground that she was unfit to work in any of the EU institutions. The applicant filed an Article 90 complaint against this decision, which the Parliament rejected. In the action before the court, the applicant alleged that her medical dossier collected by the Commission should have been used only with respect to her recruitment by the Commission. Further, the medical counsel of the Parliament should have only examined her and not inquired on her past medical history. (The EDPS brief stated that the transfer violated Regulation 45/2001. First, the data are not part of the applicant's medical dossier as former temporary agent and former contractual agent of the Commission. The procedural manual of the Commission's medical service does not indicate the ends for which medical data collected during a recruitment procedure are saved in the archive for more than 6 months, nor the conditions under which they are accessible. In opinions to the Parliament and Commission, he recommended that for candidates deemed unfit for hiring, the medical data collected during the recruitment procedure should only be held for a limited period, corresponding to the period during which it is possible to contest the data or the decision taken on the basis of the data. Further, the transfer is governed by Article 7, without prejudice to Articles 4, 5, 6 and 10. Respect of Article 7 thus does not render the transfer and ultimate use of the data legal under the Regulation in its totality. By virtue of Article 10, paragraph 1, the processing of special categories of data is prohibited and the protection of such data has, for the ECHR, a fundamental importance for exercise of the right to privacy, guaranteed by Article 8 of the Convention. The applicant did not give her consent to the transfer, in accordance with the exception foreseen in Article 10, paragraph 2. Further, the Parliament did not show that the transfer was really necessary to respect the statute, within the meaning of the Article 10(2)(b). It would have been possible to obtain the information in a less intrusive manner. Once received by the Parliament, the data were no longer being used for the purpose for which they were collected. The transfer and use of the data violated Article 4(1)(b) and (e).)

**Article 8 ECHR:** This is a fundamental right, which covers the right to secrecy of one's medical state. The transfer of that data to a third party, even another EU institution, is an interference with that right, whatever the final use. Such interference may be justified if it is "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

- In accordance with the law: Regulation 45/2001 establishes that inter-institutional transfers are foreseen. However, Article 7 is very general. Further,

Article 6 states that personal data shall only be processed for purposes other than those for which they were collected if the change of purpose has been expressly foreseen by the rules of the EU institution, which was not the case here.

- **Necessary in a democratic society:** This criterion is met if it is necessary to respond to a social imperative, and if proportionate to the legitimate end and the reasons specified are relevant and sufficient. The national authority has a limited margin of discretion. The right to privacy of medical data is protected by EU juridical order, not only to protect the private life of the sick but also to preserve their confidence in the medical body and the medical services in general. The possibility to transfer such data to another institution calls for a particularly rigorous examination. Thus the interest of the Parliament to recruit a person able to exercise his duties must be balanced against the gravity of the interference of the right of the person concerned. The interest of the Parliament to conduct the medical examination does not justify the transfer without the consent of the person concerned. The data are very sensitive, were collected nearly two years before, for a specified purpose, by an institution for which the applicant did not work. The need of the Parliament could have been met by less intrusive means.

- **Article 6 and 7:** Article 1 specifies that EU institutions protect the fundamental rights of natural persons, in particular their right to privacy with respect to processing their personal data. Thus, the provisions of the Regulation may not be read as legitimising an interference to the right to privacy. The purpose for the Commission's collection of the data was to determine the applicant's fitness to perform the duties in the Commission's post. Using them to determine her fitness for the post with the Parliament constituted a change of purpose. Each institution is an independent employer, and is autonomous in the management of its personnel. The change of purpose was not foreseen in any legal text.

**Sensitive data:** The applicant did not consent to the transfer of her data. The transfer was not "necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law," in accordance with Article 10(2)(b). The Parliament's obligation to control fitness for duty could have been achieved by less intrusive means. Nor does Article 10(3) justify the transfer.

**Damages:** 5000 euros material damages, 20.000 moral prejudice.

## 4. POST GDPR IMPLEMENTATION CASE LAWS:

### 4.1. GOOGLE CASE

In this case the Complaints were made by two organisations, noyb (Non of Your Business) and LQDN (La Quadrature du Net), in May 2018, relating to Google's forced consent to continue users data. The complaint related to Android users who, when setting up a new Android phone, were forced to follow Android's onboarding process which included forced consent for the processing of their data. Both groups

said Google had no legal basis to process the personal data of its users “ particularly for ads personalization purposes”.

GDPR requires the data controller to provide its users with the option to *opt-in* to have their data processed whereas, before the regulation's implementation, users were required to *opt-out*.

"This is the first time that the CNIL (Commission nationale de l'informatique et des libertés it means board which enforces law on data protection) has applied the new maximum penalties provided by the GDPR. The amount withheld, and the advertising of the fine, at first justified by the seriousness of the deficiencies that affect the essential principles of GDPR:

The maximum fines for GDPR are €20 million or 4% of the company's annual turnover, whichever is greater. In this case, Google could have theoretically faced a maximum fine of almost €4 billion. Google has been hit with a landmark fine €50 million GDPR fine, issued by the French policy watchdog CNIL – the largest in the GDPR's history.

The landmark fine was justified by Google's lack of action following the claim. CNIL said that the violations are continuing to this day and are ongoing violations of the GDPR.

#### **4.2. GERMAN COURTS - WHETHER AN INFRINGEMENT OF THE GDPR ALSO QUALIFIES AS UNFAIR-COMPETITIVE BEHAVIOR**

Under the Data Protection Directive (now superseded by the General Data Protection Regulation, “GDPR”), it was disputed whether a violation of the German Data Protection Law transposing the Directive could serve as a basis for anti-competition claims under the German Act Against Unfair Competition (“*Gesetz gegen den unlauteren Wettbewerb*”, “UWG”).

a. In a decision of August 7, 2018 a company asked for injunctive relief against a competing company because the competing company's website privacy policy failed to comply with the information requirements under Art. 13 GDPR. The court stressed in its decision that it is still disputed under German law, whether a violation of the GDPR can serve as a claim against a competitor under the UWG. The court refused to grant injunctive relief in that case on the grounds that the GDPR does not allow competitors to claim infringements of data protection law – only the data subjects and, under certain conditions, non-profit bodies can do this. The court concluded that, “the EU legislature did not intend to extend a similar possibility to competitors of an infringer.”

##### **Case details:**

**Date:** 08/07/2018

**Dish:** Regional Court Bochum

**Chamber:** 12th Civil Chamber

**Entscheidungsart:** Partial default and final judgment

**Docket:** I-12 O 85/18

**ECLI:** ECLI: DE: Igbo: 2018: 0807.I12O85.18.00

b. In a decision of September 13, 2018 LG Würzburg, Beschluss v. 13.09.2018 – 11 O 1741/18 UWG also relates to a claim for injunctive relief regarding a company's website privacy policy that did not comply with Art. 13 of the GDPR. The court decided that this constituted a violation of "a data protection statutory provision that is also intended to regulate market conduct in the interests of market participants and that the infringement of this data protection provision is likely to significantly prejudice the interests of consumers, other market participants or competitors" – *i.e.*, a violation of Art. 3a of the German Act Against Unfair Competition. On this basis, the court granted the injunctive relief.

#### **4.3. GOOGLE IN LANDMARK NORDIC LEGAL CASE ON THE "RIGHT TO BE FORGOTTEN."**

Finland's Supreme Court has ordered Google to remove from its search engine the personal data, including all connected URL links, of a convicted murderer.

Courts in Europe expect a surge in similar cases in the wake of the European Union's (EU) rollout of the General Data Protection Regulation (GDPR) in May.

The case is against Google in Finland was brought under both the GDPR and the country's strict personal privacy protection laws. This was no ordinary legal test case. The subject of the court order was convicted of murder, and yet the Supreme Court determined that the man's right to privacy was not diminished by his crime.

Furthermore, the court ruled that the removal of the convicted felon's data from Google's search engine didn't infringe on the public's right to information in this specific case, given that the accused was charged and found guilty of murder with "diminished responsibility," a legal annex that enhances his data protection and personal privacy rights under the GDPR and Finnish law.

Finland's Data Protection Ombudsman (DPO) took the case against Google to the country's Supreme Court after the company refused a formal written petition to have the man's personal information removed from its search engine. This information included certain facts regarding the murder case in 2012, the subsequent trial and his imprisonment.

Google, arguing its rights under freedom of speech laws, disputed the DPO's contention that the man's 11-year prison sentence constituted "inhuman suffering due to his mental impairment," or that the information pertaining to his state of health available via Google searches risked causing irreparable damage to his personal well-being.

In an earlier legal action, Google had unsuccessfully tried to have the DPO's "right to be forgotten" request rejected in Finland's Administrative Court. in the case google loses "right to be forgotten case".

#### 4.4 GDPR FINE –BARREIRO MONTIJO HOSPITAL CENTER IN PORTUGAL CASE

First fine for violation of the GDPR in Poland:

According to the DPA, the company processed the personal data of over 7 million sole-entrepreneurs for its profit-making purpose. However, the company sent individual information about this processing only to a small fraction of those persons – approx. 900,000 data subjects. Thus, the company did not provide information required by the GDPR to over 6 million people. The company argued that it did not have the email addresses of the other data subjects and that sending information to those data subjects by post would have involved a disproportionate effort, as the cost of mailing letters could be over PLN 30 million (EUR 6,978,000), which is more than the company's annual turnover. For the same reason, the company decided not to inform the data subjects via SMS. The DPA also emphasized that the main business activity and source of revenue of the company is processing personal data in a professional manner and on a large scale. As a result, the DPA reasoned that the company needed to factor into its business planning the cost of compliance with core legal obligations. It is worth noting that the data subjects in question were not consumers, but sole-entrepreneurs, whose data were collected from the official, publicly available register. It may be anticipated that in cases involving consumers, the penalties may be even higher. However, even if controllers process only business-related data, as in this case, they should also pay attention to fulfilling information duties, e.g., in relation to their business contacts, clients or vendors.

On 26 March 2019, the Polish data protection authority (DPA) announced that it has imposed its first financial penalty amounting to EUR 220,000 (approx. PLN 943,000) on a data controller in Poland for failing to comply with the provisions of the GDPR. The controller is a company that aggregates personal data from publicly available registers, such as the Central Register and Information on Economic Activity (CEIDG) and the National Court Register (KRS), for the purpose of providing company-verification services

#### 4.5. FACEBOOK BREACH IN GDPR TEST CASE.

On 28<sup>th</sup> September Facebook notified the Irish Data Protection Commissioner (DPC) about a massive data breach affecting more than 50 million of its users. The hack of the “view as” feature, which allowed users to see their profile from the perspective of an external visitor or friend, exploited an interaction of several bugs on Facebook and allowed the intruders to acquire so called “access tokens”. With these tokens, the attackers had access to personal data from the affected accounts, potentially including personal messages.

The incident is a highly salient test-case for the application of the General Data Protection Regulation (GDPR) in practice, specifically for:

**i) Notification and provision of information:** Under Article 33 of the GDPR, an entity facing a breach must notify the relevant data protection authority (DPA) within 72 hours, “where feasible”. As the vulnerability was discovered on 26 September, Facebook complied with this provision, unlike other companies have done in the past. However, the information provided by Facebook so far seems to only have delivered the very basics of what is required under the GDPR. The Irish DPC publicly urged the enterprise to submit more details so the authorities could properly assess the nature of the breach and the risk to users. Article 34 of the GDPR further requires that individuals whose personal data might have been compromised during the breach are notified without undue delay of the incident and the counter-measures that have been taken so far. Facebook implemented this by displaying a message in the feed of the affected accounts. The information provided included an initial overview on the “view as” weakness, as well as the statements that the function has been turned off and that accounts who had used it in since July 2017 had their access tokens removed, requiring a new login.

**ii) Sanctions:** The GDPR allows for sanctions against the entity that faced the breach, which depend on the sensitivity of the compromised information and the degree to which appropriate safeguards were not implemented. Since approximately five million of the affected users come from the EU, Facebook could be liable for a 1,63 billion US dollar fine if that was found to be the case. Since the exact nature of the breach is still investigated by the Irish DPC, it remains unclear to which extent the hacking was a result of negligence. In any case, the investigation might bring some further clarification on how the responsibility for the security of processing is allocated in practice, and how strictly infringements of this obligation are sanctioned. Cases like this thus offer an opportunity for other companies processing users’ personal data to learn in more detail about their security obligations under the GDPR, and provide them with examples on how to respond to a data breach. For users, the investigation also serves an important purpose: It shows them whether the security of their data is actually taken seriously. If it is not and they suffer adverse effects from that, they have the possibility to demand compensation – and

since the Irish implementation of the GDPR allows for collective redress, they could even be represented by civil society in court. On the other hand, the incident also emphasises that, even if Facebook did not act carelessly, caution about uploading personal data is always advised, as absolute safety of personal information is never certain.

This data breach is yet another example of the importance of secure and confidential storing of personal data on the Internet.

## **II. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (ORGANISED BY TOPIC)**

### **1. GENERAL**

#### **1.1. DEFINITION OF PERSONAL DATA**

**Lindquist:** The name of a person in conjunction with his/her telephone number, and information about his/her working conditions or hobbies constitute personal data.

**Tietosuojaaltuutettu:** The surname and given name of certain natural persons whose income exceeds certain thresholds, as well as the amount of their earned and unearned income, constitute personal data.

**Bavarian Lager:** Surnames and forenames may be regarded as personal data. Thus the list of names of participants in a meeting is personal data, since persons can be identified.

**Scarlet:** ISP addresses are protected personal data because they allow the related users to be precisely identified.

**M:** The data relating to the applicant for a residence permit included in the minute (applicant's name, DOB, nationality, gender, ethnicity, religion and language) constitute personal data. The legal analysis in the minute may contain personal data but it does not in itself constitute such data. The legal analysis is not information relating to the applicant, but at most, in so far as not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation. This interpretation is consistent with the language of Article 2(a) and the objective and general scheme of Directive 95/46.

**Schwartz:** Fingerprints constitute personal data, as they objectively contain unique information about individuals, which allows them to be identified with precision.

**Worten:** Data contained in the record of working time concerning, in relation to each worker, the daily work periods and rest periods, constitute personal data because they represent "information relating to an identified or identifiable natural person."

**Englebert:** Data collected by private detectives relating to persons acting as estate agents concern identified or identifiable natural persons, and therefore constitute personal data.



Rynes: The image of a person recorded by a camera constitutes personal data because it makes it possible to identify the person concerned.

Client Earth: The information as to which expert is the author of each comment made by the external experts constitutes information, which falls within the scope of personal data. The fact that the information is provided as part of a professional activity does not mean that it cannot be characterized as personal data. The concepts of personal data and data relating to private life are not to be confused. The claim that the information concerned does not fall within the scope of private life is therefore ineffective.

Likewise, the fact that both the identity of the experts concerned and the comments submitted on the draft guidance were made public on the EFSA website does not mean such data cannot be characterized as personal data.

Finally, characterization of information relating to a person as personal data does not depend on whether the person objects to the disclosure of that information.

Bara: Tax data transferred are personal data, since they are “information relating to an identified or identifiable natural person.”

Nikolaou: The information published in the press release was personal data, since the data subject was easily identifiable, under the circumstances. The fact that the applicant was not named did not protect her anonymity.

Jordana: The first and last names of the persons on the reserve list and the officials mentioned in the individual decisions of appointment to grade A6 can be considered to fall within the personal data definition.

McCullough: Surnames are personal data and therefore are protected by Regulation 45/2001. The fact that the members of Cedefop’s decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, and that the surnames were published in the OJ or on the internet, does not affect the characterization of the surnames as personal data.

## **1.2. DEFINITION OF PROCESSING**

Lindquist: The operation of loading personal data on an Internet page must be considered to be processing.

Tietosuojavaaltuutettu: The collection, publication, transfer on a CD-ROM and by text messaging all constitute processing of personal data. This includes personal data that have already been published in unaltered form in the media, as cooperation referred to in Article 2(b) must be classified as processing also where they exclusively concern material that has already been published in unaltered form in the media. A general derogation from the application of the Directive in such a case would largely deprive the Directive of its effect.

Bavarian Lager: Communication of personal data in response to a request for access to documents constitutes processing.

Bonnier: Communication of name and address sought by applicants constitutes processing of personal data.

Google: The operation of loading personal data on an Internet page must be considered processing (Lindquist). In exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine “collects” such data which it subsequently “retrieves”, “records” and “organizes” within the framework of its indexing programmes, “stores” on its servers and, as the case may be, “discloses” and “makes available” to its users in the form of lists of search results, which constitute processing, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. This finding is not affected by the fact that those data have already been published on the Internet and are not altered by the search engine. It is not necessary that the personal data be altered. While alteration of personal data constitutes processing under Article 2(b), the other operations mentioned there do not require the alteration of personal data.

The processing done by the search engine operator is distinguished from and in addition to that done by publishers of websites, consisting in loading those data on an Internet page.

Schwartz: Taking and storing fingerprints constitute processing.

Bara: Both the transfer of the data by ANAF, and the subsequent processing by CNAS, constitute processing of personal data.

Weltimmo: The operation of loading personal data on an Internet page constitutes processing.

Esch-Leonhardt: Inclusion of the letters in the personal files constitutes processing by saving data in a personal data filing system as provided in Article 2(a), (b) and (c) of Regulation 45/2001.

Nikolaou: 1. the leak (unauthorised transmission of personal data to a journalist by someone inside OLAF) and 2. the publication of a press release each constitute processing of personal data. Jordana: Transfer of the data constitutes processing.

### **1.3. DEFINITION OF CONTROLLER**

Google: The search engine operator determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of the activity and is thus a controller. It would be contrary not only to the clear wording of Article 2(d) and to its objective, which is to ensure through a broad definition of the concept of controller, effective and complete protection of data subjects, to exclude the operator of a search engine on the ground that it does not

exercise control over the personal data published on the web pages of third parties. Moreover, the activity of search engines plays a decisive role in the overall dissemination of the personal data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published. The search results also provide a structured overview of the information relating to that individual that can be found on the Internet, enabling them to establish a detailed profile of the data subject. The fact that publishers of websites have the option of indicating to operators by means of exclusion protocols that they wish some information published on their site to be excluded from search engines' automatic indexing does not mean if publishers do not so indicate, the operator of the search engine is released from responsibility for its processing of personal data.

Rynes: Arts. 7(f), 11(2) and 13(1)(d) and (g) make it possible to take into account the legitimate interests of the controller in protecting the property, health and life of his family and himself.

#### **1.4. LEGAL PERSONS**

Schecke: Legal persons can claim protection of Articles 7 and 8 of the CFR only insofar as the official title of a legal person identifies one or more natural persons. Here, the name of the legal person directly identifies natural persons who are its partners.

Bank Austria: A legal person does not belong to the circle of persons which Regulation 45/2001 is intended to protect. That conclusion cannot be invalidated by the applicant's arguments of its supposed obligations towards directors and employees under Member State law, given that they consist of unsubstantiated contentions. These arguments are not sufficient to demonstrate the applicant's personal interest in relying on a breach of Regulation 45/2001.

#### **1.5. SENSITIVE PERSONAL DATA**

Lindquist: Reference to the fact that an individual has injured her foot and is on medical leave constitutes personal data concerning health within the meaning of Article 8(1), as that provision must be given a wide interpretation so as to include all aspects, both physical and mental, of the health of an individual.

Esch-Leonhardt: Inclusion of a letter concerning an ECB staff member's use of internal e-mail to transmit union information in his personal file does not infringe Article 10(1) as it concerns data which the person himself has manifestly made public within the meaning of Article 10(2)(d).

Egan & Hackett: The argument that release of names of former MEP assistants would reveal their political opinions and therefore constitute sensitive data was not substantiated and cannot make up for the fact that the contested decision failed to

show why disclosure would specifically and effectively undermine their right to privacy within the meaning of Article 4(1)(b) of Regulation 45/2001.

V: The applicant did not consent to the transfer of her medical file by the Commission to the European Parliament. The transfer was not "necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law," in accordance with Article 10(2)(b). The Parliament's obligation to control fitness for duty could have been achieved by less intrusive means. Nor does Article 10(3) justify the transfer.

## **1.6. CONSENT**

Schecke: The legislation at issue (EU rules on financing under CAP and publication on internet) does not seek to base the personal data processing for which it provides on consent of the beneficiaries concerned. Rather, it provides that they are to be informed. Thus, processing is not based on their consent. Therefore, it is necessary to analyse whether interference is justified under CFR Article 52(1).

Schwartz: It is essential for citizens of the EU to own a passport in order to travel to a third country, and a passport must contain fingerprints. Therefore, citizens are not free to object to processing of their fingerprints, and thus persons applying for passports cannot be deemed to have consented to that processing.

## **1.7. NECESSITY/PROPORTIONALITY**

Huber: Directive 95/46 is intended to ensure an equivalent level of data protection in all Member States, to ensure a high level of protection in the EU. The concept of necessity in Article 7(e) cannot have a meaning which varies among Member States. Thus, it is a concept which has its own independent meaning in EU law, and must be interpreted in a manner which fully reflects the objective of Directive 95/46.

Under EU law, the right of free movement of a Member State national is not unconditional, but may be subject to limitations and conditions imposed by the Treaty and implementing rules. Legislation provides that a Member State may require certain documents to be provided to determine the conditions of entitlement to the right of residence. Thus, it is necessary for a Member State to have relevant particulars and documents available to it in order to ascertain whether a right of residence in its territory exists. Use of a register to support authorities responsible for the application of the legislation on the right of residence is, in principle, legitimate. However, the register must not contain any information other than what is necessary for that purpose, and must be kept up to date. Access must be restricted to the responsible authorities. The central register could be necessary if it contributes to a more effective application of that legislation. The national court should decide whether these conditions are satisfied. Only anonymous information is required for statistical purposes. Scarlet: The contested filtering system (to detect e-communications which use file sharing software, with a view to preventing

copyright infringement) may infringe the right to protection of personal data of the ISP's customers, as it would involve a systematic analysis of all content and the collection and identification of users' IP address from which unlawful content on the network is sent.

Schwartz: Storage of fingerprints on a highly secure storage medium is likely to reduce risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders, although it is not wholly reliable. Thus, it is appropriate.

The action involves taking prints of two fingers, causing no physical or mental discomfort, plus a facial image. The only real alternative to fingerprints is iris scan, the technology of which is not yet as advanced as fingerprint recognition. Thus, no apparent alternative exists that is sufficiently effective and less of a threat to the protected rights.

Concern that data may be centrally stored and used for other purposes (e.g. criminal investigation or to monitor the person indirectly) does not affect the validity of the Regulation, which provides only for preventing illegal entry into the EU.

Worten: The referring court must verify that the personal data contained in the record of working time are collected in order to ensure compliance with the national legislation relating to working conditions and that the processing of those data is necessary for compliance with a legal obligation to which Worten is subject and the performance of the monitoring task entrusted to the national authority responsible for monitoring working conditions. Only the grant of access to authorities having powers of monitoring could be considered to be necessary within the meaning of Article 7(e). Further, the obligation to provide immediate access to the record could be necessary if it contributes to the more effective application of the legislation relating to working conditions. It is for the referring court to decide whether this requirement is necessary.

Penalties must respect the principle of proportionality.

Client Earth: No automatic priority can be conferred on the objective of transparency over the right to protection of personal data. However, the information was necessary to ensure the transparency of the process of adoption of a measure likely to have an impact on the activities of economic operators, in particular, to appreciate how the form of participation by each expert might have influenced the content of that measure. Transparency of the process followed by a public authority for adoption of a measure contributes to the authority acquiring greater legitimacy in the eyes of the persons to whom the measure is addressed and increasing their confidence in that authority, and ensuring the authority is more accountable to citizens in a democratic system. Obtaining the information at issue was therefore necessary so that the impartiality of each expert in carrying out their tasks as scientists in the service of EFSA could be ascertained. Thus, a public interest justified the disclosure of the information at issue, in accordance with Article 8(a) and (b).

Esch-Leonhardt: The ECB may be entitled to consider that inclusion of letters concerning ECB staff members' use of internal e-mail to transmit union information in their personal file is necessary for the performance of their contract of employment. Insofar as the letters send a warning to those concerned, they relate to their administrative status and may become relevant for a report on their conduct in the service; thus it is appropriate to include them. A shortened version, omitting reference to relations between those concerned and the trade union, would not be sufficient for proper management of personal files. The fact that the staff in question contravened rules on the use of the ECB's internal email system by using it, as members of a trade union, for purposes of that union, and not for gainful purposes, is liable to influence the assessment of their conduct in the service.

### **1.8. SECURITY**

Worten: Article 17(1) requires controllers (not Member States) to adopt technical and organizational measures which, having regard to the state of the art and cost of their implementation, are to ensure a level of security appropriate to the risks represented. The obligation under national law to provide the national authority responsible for monitoring working conditions with immediate access to the record of working time does not imply that the data must be made accessible to persons not authorised for that purpose (as Worten claimed). Rather, Worten must ensure that only those persons duly authorised to access the personal data in question are entitled to respond to a request for access from a third party. Thus, Article 17(1) is not relevant here.

### **1.9. DEROGATIONS**

Englebert: The activity of a body such as IPI (a professional body responsible for ensuring compliance with the rules governing the profession of estate agent which is a regulated profession in Belgium, through investigating and reporting breaches of those rules) corresponds to "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions" and is capable of coming under that exception. The directive does not prevent such a professional body from having recourse to private investigators. Thus, if a Member State has chosen to implement the exception, then the professional body and private detectives may rely on it and are not subject to the obligation to inform the data subject. However, if the Member State has not implemented the exception, the data subjects must be informed.

Rules on access to a regulated profession form part of the rules of professional ethics, therefore investigations concerning the acts of persons who breach those rules by passing themselves off as estate agents are covered by the exception in Article 13(1)(d).

Bara: Article 13(1)(e) and (f) provide exceptions for important economic or financial interest of a Member State and monitoring, inspection or regulatory function, respectively. However, Article 13 expressly requires that such restrictions are imposed by legislative measures. Here, however, the transfer from the Member State tax authority to the health insurance authority on the data subject's declared income was made on the basis of a protocol between the two authorities, which is not a legislative measure, and is not subject to an official publication. Thus, the conditions of Article 13 were not complied with.

## **1.10. NON-CONTRACTUAL LIABILITY**

Nikolaou: The normal rule is that the burden of proof is on the applicant to establish: i) the illegal action of an institution; ii) damages; iii) proof that the damages were caused by the illegal action of the institution. However, the burden of proof shifts to the institution when a fact giving rise to damages could have resulted from various causes, and the institution has not introduced any element of proof as to which was the true cause, even though it was best placed to do so. The Court concluded that the OLAF staff member leaked information (including PD) to a journalist, which were published, and OLAF's press release confirmed the veracity of facts (including PD) that had been mentioned in several press articles.

A violation of Regulation 45/2001 qualifies as an illegal act of an institution conferring rights on an individual. The objective of the Regulation is to confer such rights on data subjects.

A leak of personal data is necessarily a grave and manifest violation. The Director has a margin of appreciation on prevention, but here no showing was made regarding the exercise of the margin.

OLAF gravely and manifestly exceeded the limits of its discretion in the application of Article 5(a) and (e), which was sufficient to engage the responsibility of the Community.

3000 euros damages were awarded.

V: 5000 euros material damages, 20.000 moral prejudice, were awarded.

## **2. DATA SUBJECT RIGHTS**

### **2.1. INFORMATION**

Bara: The requirement of fair processing laid down in Article 6 of Directive 95/46 requires a public administrative body to inform the data subjects of the transfer of their data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data. National law required the transfer of data necessary to certify that the person concerned qualifies as an insured person to CNAS. However, these do not include data relating to income, since the law recognises the right of persons without a taxable income as qualifying

as insured. Thus, the national law cannot constitute “prior information” under Article 10 of Directive 95/46 (information requirement where data is collected from the data subject), enabling the controller to dispense with his obligation to inform the data subject of the recipients of the income data, and the transfer therefore violated Article 10.

Article 11 (information requirement where data is not collected from data subject) requires that specified information be provided to the data subject, including the categories of data concerned and the existence of the rights of access and rectification. Thus, the data subjects should have been informed of the processing by CNAS and of the categories of data concerned, but CNAS did not so inform them. The Protocol between the two agencies does not establish grounds for derogating from this requirement, either under Article 11 or 13 of the Directive.

## 2.2. ACCESS

Rijkeboer: The right of access is necessary to enable the data subject to exercise his other rights (rectification, blocking, erasure, and notify recipients of same; object to processing or request damages). The right must of necessity relate to the past, otherwise the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for damages. Member States have some freedom of action in implementing the Directive, but it is not unlimited. Setting of a time limit on the right of access must allow the data subject to exercise his rights. It is for the Member States to fix a time limit for storage of information on the recipients and the content of the data disclosed, and to provide access to that information which constitutes a fair balance between the interest of the data subject in exercising his rights and the burden on the controller to store that information. In the present case, limiting storage of information on recipients and content to one year, while the basic data is stored much longer, does not constitute a fair balance, unless it can be shown that longer storage would constitute an excessive burden.

M: Regarding the right of access, protection of the fundamental right to respect for private life means that the person may be certain that the personal data concerning him are correct and that they are processed lawfully. It is in order to carry out the necessary checks that the data subject has, under Article 12(a), a right of access, which is necessary to obtain rectification, erasure or blocking of his data (Article 12(b)). The legal analysis is not in itself liable to be the subject of a check of its accuracy by the applicant and rectification, while the facts are. Moreover, the right of access is not designed to ensure the greatest possible transparency of the decision-making process of public authorities and to promote good administrative practices (as is the case for the right of access to documents).

To comply with the right of access under Article 12(a) and Article 8(2) of CFR, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and



to check that they are accurate and processed in compliance with the Directive. He need not be given a copy of the documents.

X: Article 12(a) of Directive 95/46 does not require Member States to levy fees when the right of access to personal data is exercised, nor does it prohibit the levying of such fees as long as they are not excessive. Access must be without constraint, without excessive delay and without excessive expense. The fees should be fixed at a level which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular his right to have the data communicated to him in an intelligible form, and on the other, the burden which the obligation to communicate such data represents for the controller. The fees may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access, and it should not exceed the cost of communicating such data.

### **2.3. ERASURE**

Google: A supervisory authority or judicial authority may order a search engine operator to remove a link from a list of results without presupposing the previous or simultaneous removal of the underlying information from the web page on which it was published. Requiring the data subject to obtain erasure from web pages would not provide effective and complete protection of the data subject, especially because publishers may not be subject to EU data protection law or publication may be carried out “solely for journalistic purposes” and thus benefit from the derogation. Further, balancing would be different for processing by a search engine and processing by a web publisher.

The search engine operator must erase the information and links concerned in the list of results if that information appears, having regard to all circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine. Here, having regard to the sensitivity for the data subject’s private life of the information contained in announcements and the fact that initial publication occurred 16 years before, the data subject has established that the links should be removed.

## **3. BALANCING FUNDAMENTAL RIGHTS**

### **3.1. PROTECTION OF PROPERTY AND AN EFFECTIVE REMEDY**

Promusicae: The requirements of protection of different fundamental rights must be reconciled, namely the right to respect for private life on the one hand and rights to protection of property and an effective remedy on the other hand. Directive 2002/58 provides rules determining in what circumstances and to what extent personal data processing is lawful and what safeguards must be provided.

LSG: The decision refers to of Promusicae decision regarding balancing fundamental rights. That decision did not rule out the possibility that Member States may place ISP under a duty of disclosure. An ISP provides a service which enables users to infringe copyright by providing the connection.

Scarlet: The injunction to install the contested filtering system did not respect the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information.

Bonnier: The national legislation in question requires, for an order for disclosure of the data in question to be made, that there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into a copyright infringement and that the reasons for the measure outweigh the potential harm to the person affected. Thus, it enables the national court seised of an application for an order for disclosure of personal data to weigh the conflicting interests involved, and thereby in principle ensures a fair balance between protection of intellectual property rights and protection of personal data.

### **3.2. FREEDOM OF EXPRESSION**

Lindquist: Data protection and freedom of expression must be balanced against each other, and the regime of the Directive provides in itself multiple mechanisms allowing a balancing of the different fundamental rights to be carried out. Therefore it is not a disproportionate violation of the principle of freedom of expression.

### **3.3. ACCESS TO DOCUMENTS**

Bavarian Lager: The General Court erred in limiting the application of the exception in Article 4(1)(b) to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the case law of the European Court of Human Rights, without taking into account the legislation of the EU concerning the protection of personal data, particularly Regulation 45/2001. It disregarded the wording of the Article, which is an indivisible provision and requires that any undermining of privacy and the integrity of the individual must always be examined and assessed in conformity with the EU data protection legislation. The Article establishes a specific and reinforced system of protection of a person whose personal data could, in certain cases, be communicated to the public.

Recital 15 of Regulation 45/2001 indicates legislative intent that Article 6 TEU and thereby Article 8 ECHR should apply where processing is carried out in the exercise of activities outside the scope of Regulation 45/2001 (Titles V and VI of pre-Lisbon TEU). Such reference was unnecessary for activities within the scope of Regulation 45/2001. Thus, where a request based on Regulation 1049/2001 seeks access to documents including personal data, Regulation 45/2001 becomes applicable in its

entirety, including Articles 8 and 18. The General Court erred in dismissing the application of Article 8(b) and 18 of Regulation 45/2001, and its decision does not correspond to the equilibrium, which the legislator intended to establish between the two Regulations.

The Commission was right to verify whether the data subjects had given their consent to disclosure of personal data concerning them. By releasing the expurgated version of the minutes, with the names of 5 participants removed (three could not be contacted, two objected), the Commission did not infringe Regulation 1049/2001 and complied with its duty of openness. By requiring that regarding these five persons, the applicant establish the necessity for those personal data to be transferred, the Commission complied with the provisions of Article 8(b) of Regulation 45/2001. As no necessity was provided, the Commission was not able to weigh up the various interests of the parties concerned, nor to verify whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by Article 8(b).

Client Earth: Where an application is made seeking access to personal data, the provisions of Regulation 45/2001 (particularly Article 8(b)) become applicable in their entirety. Under Article 8(b), personal data may generally be transferred only if the recipient establishes necessity and if there is no reason to assume that the transfer might prejudice the legitimate interests of the data subject. Thus, the transfer is subject to these two cumulative conditions being satisfied. The applicant must establish the first condition, and the institution must determine whether there is such reason. If there is no such reason, the transfer must be made; if there is such reason, the institution must weigh the various competing interests in order to decide on the request.

The consideration that disclosure was likely to undermine the privacy and integrity of the experts concerned is a consideration of a general nature not otherwise supported by any factor specific to the case. Disclosure would have made it possible for suspicions of partiality to be dispelled or allowed the experts to dispute the merits of those allegations. If a general consideration, unsupported by evidence, were to be accepted, it could be applied to any situation where an EU authority obtains experts opinions, contrary to the requirement that exceptions to the right of access to documents must be interpreted strictly. Thus, the conditions required by Article 8(b) were satisfied.

Jordana: Article 4(1)(b) of Regulation 1049/2001 is indivisible, and requires that the violation of private life and the integrity of the individual are always analysed in conformity with the right to protection of personal data. Thus it establishes a specific regime where personal data may be communicated to the public. Since this case concerns the processing of personal data, the request must be analysed under Regulation 45/2001. In rejecting the application for access to documents, the Commission had failed to apply Regulation 45/2001 in its analysis, and thus erred.

Dennekamp I: Regulation 1049/2001 and Regulation 45/2001 do not contain any

provisions granting one primacy over the other, therefore full application of both should, in principle, be ensured.

Where a request based on Regulation 1049/2001 seeks access to documents containing personal data, Regulation 45/2001 becomes applicable in its entirety, including Article 8. The applicant cannot claim that the processing he requested was lawful on the basis of Article 5(b) and this suffices, since Article 8(b) applies without prejudice to Article 5.

In order to obtain disclosure of the personal data contained in the documents, the applicant would have had to demonstrate, by providing express and legitimate justifications, the necessity for the requested personal data to be transferred, so that the Parliament could weigh up the various interests of the parties concerned and determine whether legitimate interests of MEPs might be prejudiced by the transfer. The applicant failed to establish why he needed the names to obtain his objectives. He did not explain with express arguments and justifications in what respect the transfer of the data was necessary to satisfy the public interest which he invoked, nor that the transfer would have been proportionate to his aims.

Further, the Parliament was not required to weigh the interests invoked by the applicant against those of MEPs, or to determine whether there was any reason to assume that the legitimate interests of those MEPs might have been prejudiced by such transfer. Thus, no manifest error that the Parliament might have made in weighing up interests has any bearing in this case on the lawfulness of the decision.

Article 4(1)(b) is an indivisible provision requiring the institution concerned always to examine and assess any undermining of privacy and the integrity of the individual in conformity with Regulation 45/2001.

*Egan & Hackett*: The Parliament systematically took the view that the public should not have access to documents revealing the identity of former MEP assistants. It did not carry out an examination to show that the access would specifically and effectively undermine their privacy within the meaning of the provisions in question, nor did it verify whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. Thus, it failed to show to what extent disclosure would specifically and effectively undermine the right to privacy.

*Dennekamp II*: If the applicant has established necessity, and the institution decides there is no reason to assume that data subject's legitimate interests may be prejudiced, the data may be transferred and the documents are to be made available to the public. To fulfill the condition of necessity under that article, an applicant for access to documents containing personal data must establish that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and it is proportionate to that objective, which means the applicant must submit express and legitimate reasons to that effect. This strict interpretation cannot be regarded as creating a broad exception to the fundamental right of access to documents, which would result in an unlawful restriction of that right. Rather, it reconciles two fundamental yet opposing rights, the institution being

required also to examine whether the legitimate interests of the data subjects might be prejudiced by the transfer. The general nature of the justification for transfer has no direct effect on whether the transfer is necessary for the purposes of attaining the applicant's aim. Here, the applicant made two arguments to establish necessity. First, that necessity was based on the right to information and freedom of expression. These are not sufficient to establish that the transfer is the most appropriate of the possible measures for attaining the objective, or that it is proportionate to that objective. Moreover, the applicant did not make clear in what respect transferring the names of the MEPs participating in the scheme was the most appropriate measure for attaining the objective he had set for himself. He merely asserted that the measures designed to provide public control over public expenditure in the context of the additional pension scheme, like the discharge procedure, did not protect the fundamental right to information and to communicate it to the public. From this it cannot be determined in what respect the transfer would be the most appropriate measure, or how it is proportionate.

Second, the applicant argued that the transfer of personal data is necessary to determine whether MEPs' voting behavior regarding the additional pension scheme is influenced by their financial interest, and disclosure of all the names of the MEPs participating in the scheme would be the only way for the public to hold its representatives accountable for their actions in relation to the scheme. The court agreed that the transfer is the only measure by which the applicant's aim can be attained; no other measure is capable of ensuring that MEPs facing a potential conflict of interest are identified. Further, it is proportionate for this purpose.

The EU institution or body in receipt of the application must refuse the transfer if there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced. MEPs as public figures have chosen to expose themselves to scrutiny by third parties, particularly the media and general public, even if such choice in no way implies that their legitimate interests must be regarded as never being prejudiced by a decision to transfer their data. Thus, they have generally already accepted that some of their personal data will be disclosed to the public. That must be taken into account when assessing the risk of prejudice to their legitimate interests. Particular consideration should be given to the link between the personal data at issue and their mandate, and to the legal and financial commitment of the EP to the scheme. In view of the importance of the interests invoked here, which are intended to ensure the proper functioning of the EU by increasing the confidence that citizens may legitimately place in the institutions, the legitimate interests of the MEPs who are members of the scheme cannot be prejudiced by the transfer of personal data at issue.

An institution which refuses access on the ground of prejudice to legitimate interests must state reasons for invoking such interests. The institution must explain how disclosure of a document could specifically and actually undermine the interest protected by the exception. The explanation cannot consist of a mere assertion that access would undermine privacy. Examination of the specific and actual nature of

the undermining of the interest under Article 4(1)(b) of Regulation 1049/2001 is indissociable from the assessment of the risk that the legitimate interests of the data subject referred to in Article 8(b) of Regulation 45/2001 which, through the disclosure to the public, might be prejudiced by the transfer of personal data.

McCullough: The applicant cannot be deemed to have proved the necessity of having the personal data at issue transferred. The only justification provided was to supplement his written defence before the Greek Examining Magistrate. Applicant did not provide any information or justification as to how the submission of the requested documents containing that data would affect the Greek proceedings, the risks to which he would be exposed in procedural terms, and the merits of his defence if the documents were not submitted to the Greek Magistrate.

Exceptions under Article 4 must be interpreted and applied strictly. An institution refusing access must explain how disclosure of that document could specifically and actually undermine the interest protected by the exception. The fact that a document concerns an interest protected by an exception is not of itself sufficient to justify application of that exception. Rather, it is necessary for the institution to have previously determined (1) that the document would specifically and actually undermine the protected interest and (2) that the risk of the protected interest being undermined is reasonably foreseeable and not purely hypothetical. The institution must explain how granting access to the document could specifically and actually undermine the interest protected by the exception under Article 4(1)(b).

Here, Cedefop simply states that the persons concerned are protected as individuals and any access would lead to a serious violation of the privacy and integrity of the individual as they clearly demonstrated the opinions and views of the members on the subject matters discussed. However, Cedefop neither carried out an examination demonstrating that granting access to those documents would specifically and actually undermine the privacy of those members within the meaning of Article 4(1)(b), nor verified whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical. It is not apparent how the opinions and views expressed could fall within the sphere of their privacy, since those meetings were professional.

#### **4. TRANSFERS**

Lindquist: The publication on the Internet did not constitute a transfer, as an Internet user would have to connect to the Internet and personally carry out the necessary actions to consult those pages. Mrs. Lindquist's Internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access. There is no transfer of data to a third country within the meaning of Article 25 when an individual in a Member State loads personal data onto an internet page which is stored with his/her hosting provider in that or another Member State, thereby making the data accessible to anyone who connects to the internet, including people in a third country.

Dennekamp II: Articles 7-9 of Regulation 45/2001 precisely limit the possibility of transferring personal data so as to make it subject to strict conditions which, if not fulfilled, prohibit any transfer. Those conditions always include the necessity of the transfer in the light of various aims.

#### **4.1. APPROPRIATE LEGAL BASIS**

PNR:

- Adequacy decision: Requirements for transfer were based on a statute enacted by the USA in November 2001 and implementing regulations adopted thereunder, which concern enhancement of security and conditions under which persons may enter and leave the USA, fighting against terrorism and transnational crime. Thus, the transfer of PNR data is processing concerning public security. Even though PNR data are initially collected in the course of commercial activity, the processing addressed in the adequacy decision concerns safeguarding public security and law enforcement. The facts that the data are collected by private operators for commercial purposes and that those operators arrange for the transfer of the data to a third country does not prevent that transfer from being regarded as processing excluded from the Directive's scope. Thus, it falls within the first indent of Article 3(2) of the Directive, which excludes from the Directive's scope data protection in the course of activities provided for by Titles V and VI of the EU Treaty. Thus the adequacy decision is annulled.
- Agreement: Article 95 of the EC Treaty (internal market) in conjunction with Article 25 of the Directive (transfers to third countries ensuring adequacy) do not justify EU competence to conclude the Agreement. The agreement relates to the same transfers as the adequacy decision, and thus processing operations are outside the scope of the Directive. The Council decision approving the conclusion of the agreement between the EU and the US on the processing of PNR data is annulled.

#### **4.2. ADEQUATE LEVEL OF PROTECTION**

Schrems: The word “adequate” in Article 25(6) signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed by the EU legal order. However, it requires the third country to ensure, by reason of its domestic law or international commitments, a level of protection of fundamental rights and freedoms *essentially equivalent* to that guaranteed by the EU by virtue of Directive 95/46 read in light of the CFR, otherwise that protection could be easily circumvented by transfers. Thus, the legal order of the third country covered by a Commission adequacy decision must have the means to ensure protection essentially equivalent to that guaranteed within the EU. When examining the level of protection afforded by a third country, the Commission must assess the content of the applicable rules resulting from domestic law or international commitments and the practice designed to ensure compliance. Also, in light of the fact that the level of

protection ensured by the third country is liable to change, the Commission must, after adopting an adequacy decision, check periodically whether the adequacy finding remains factually and legally justified. Account must be taken of the circumstances that have arisen after the adoption of the decision. The Commission's discretion as to adequacy is reduced and is subject to strict scrutiny, in view of the important role played by data protection in the light of the fundamental right to respect for private life and the large number of persons potentially concerned by transfers.

#### **4.3. SAFE HARBOUR**

Schrems: US public authorities are not required to comply with safe harbor principles. Decision 2000/520 specifies that safe harbor principles may be limited to the extent necessary to meet national security, public interest or law enforcement requirements, or statute, regulation or case law. Self-certified US organisations receiving personal data from the EU are thus bound to disregard safe harbor principles when they conflict with US legal requirements. Decision 2000/520 does not contain sufficient findings regarding US measures which ensure adequacy by reason of domestic law or international commitments. Rather, it enables interference with fundamental right to respect for private life of persons whose personal data is or could be transferred from the EU to the US.

The Decision does not contain any finding regarding US rules intended to limit the interference when they pursue legitimate objectives such as national security, nor refer to effective legal protection against such interference. FTC procedures and private dispute resolution mechanisms concern compliance with safe harbor principles (against US organisations) and cannot be applied with respect to measures originating from the State. Moreover, the Commission found that US authorities could access the personal data transferred and process it in a way incompatible with the purposes for which it was transferred, and beyond what was strictly necessary and proportionate for the protection of national security, and data subjects had no redress regarding their rights of access, rectification and erasure. Legislation permitting public authorities to have generalized access to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access, rectification or erasure of his own personal data does not respect the essence of the fundamental right to effective judicial protection.

Thus, Article 1 of the Decision does not ensure adequacy and the decision is consequently invalid.

Articles 1 and 3 are inseparable from 2 and 4 and the annexes, thus the entire Decision 2000/520 is invalid.



## **5. REGULATION 45/2001**

### **5.1. SCOPE**

Egan & Hackett: Neither Article 2(3) of Regulation 1049/2001, nor Article 3(2) of Regulation 45/2001, nor any other provision, contains any restriction such as to exclude from their respective scopes documents which were, but are no longer, available.

### **5.2. LAWFULNESS**

Nikolaou: The leak constitutes unlawful processing in violation of Article 5 of Regulation 45/2001 because it was not authorized by the data subject, not necessary under the other sub-paragraphs and it did not result from a decision by OLAF. Even though OLAF has a margin of discretion on transmissions, here it was not exercised because the leak is an unauthorized transmission. OLAF is best placed to prove how the leak occurred and that the Director of OLAF did not violate his obligations under Article 8(3) of Regulation 1073/99. In the absence of such proof, OLAF (the Commission) must be held responsible. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality.

Publication of the press release was not lawful under Article 5(a) and (b) because the public did not need to know the information published in the press release at the time of its publication, before the competent authorities had decided whether to undertake judicial, disciplinary or financial follow-up.

## **6. DIRECTIVE 95/46**

### **6.1. SCOPE**

Rechningshof: Applicability of Directive 95/46 cannot depend on whether the specific situations at issue have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty (free movement of workers). The EU system of data protection has a wide scope, is defined in very broad terms, and does not depend on whether, in every specific case, the processing of personal data has a connection to the free movement between the Member States. A contrary interpretation could make the limits of the field of application of the Directive unsure and uncertain. The system consists of checks and balances in which processing of personal data is subject to a number of conditions and limitations.

Lindquist: Loading personal data on an Internet page is processing by automatic means.

Huber: Article 3(2) excludes from the scope of Directive 95/46 the processing of personal data concerning public security, defense, and criminal law activities. Thus, in this case, only processing for a purpose relating to the right of residence and for statistical purposes falls within the scope of Directive 95/46.

Tietosuojavaltuutettu: Only two exceptions to scope exist, which are set forth in Article 3(2). The first indent states that security and criminal law are activities of the state. The second indent states that processing by a natural person in the course of a purely personal or household activity concerns activities in the course of private or family life of individuals. Activities (c) and (d) are activities of private companies, and are not within the scope of Article 3(2). A general derogation from application of the Directive in respect of published information would largely deprive the Directive of its effect. Thus activities (a) and (b) are also not within the scope of Article 3(2).

Rynes: Video surveillance involving the recording and storage of personal data falls within the scope of the Directive, since it constitutes automatic data processing.

## 6.2. LAWFULNESS

ASNEF: The second condition of Article 7(f) of Directive 95/46 (the interests of the controller or recipients must not be overridden by the fundamental rights and freedoms of the data subject) necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case. In relation to the balancing, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources. The processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and recipients, which is a more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the CFR, and must be properly taken into account in the balancing. However, it is no longer a precision within the meaning of Article 5 if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing the result of the balancing thereby not allowing a different result by virtue of the particular circumstances of an individual case.

Google: The non-compliant nature of processing may arise from a breach of any conditions of lawfulness imposed by the directive, including data quality and legitimacy. Here, the grounds for legitimacy were those in Article 7(f), which permits processing where necessary for the purposes of the legitimate interests pursued by the controller or third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights of the data subject, requiring a balancing of interests. The balancing provided in Article 14 allows account to be taken of all circumstances surrounding data subject's particular situation.

- Interest of the data subject: search of an individual's name enables any internet user to obtain through a list of results a structured overview of the information relating to the data subject that can be found on the internet, potentially concerning a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or only with great difficulty, therefore enabling a

detailed profile. The interference with the rights of the data subject are heightened because of the important role played by the internet and search engines in modern society.

- Interests of search engine: These are economic interests, which cannot justify the potential seriousness of the interference with the data subject's rights.
- Interests of internet users: The data subject's rights generally override those of internet users, but the balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, which may vary by the role played by the data subject in public life. The interference may be justified by the preponderant interests of the general public in having access to the information.

### **6.3. ESTABLISHMENT OF THE CONTROLLER**

Google: Google Spain, a subsidiary of Google Inc. on Spanish territory, is an "establishment" within the meaning of Article 4(1)(a) because it engages in the effective and real exercise of activity through stable arrangements in Spain.

The processing of personal data by the controller is also "carried out in the context of the activities" of an establishment, even though Google Spain is not involved in the processing at issue (carried out exclusively by Google Inc.) but rather only in advertising in Spain. Article 4(1)(a) does not require that the processing in question be carried out "by" the establishment concerned, but only "in the context of the activities" of the establishment. In light of objective of effective protection of fundamental rights, those words cannot be interpreted restrictively. The activities of the search engine and those of its establishment in the Member State are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine economically profitable and that engine is the means enabling those activities to be performed.

Weltimmo: Article 4(1)(a) of Directive 95/46 permits the application of data protection law of a Member State other than the Member State in which the controller is registered, insofar as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity, even minimal, in the context of which the processing is carried out. To establish whether the controller has an establishment in that Member State, both the degree of stability of the arrangements and the effective exercise of activities in the other Member State must be interpreted in light of the specific nature of the economic activities and provision of services concerned, particularly for undertakings offering services exclusively over the internet. The presence of only one representative can suffice to constitute a stable arrangement if he/she acts with a sufficient degree of stability through the presence of the necessary equipment for the provision of the specific services concerned in the Member State. Further, the concept of "establishment" extends to any real and effective activity, even a minimal one, exercised through stable arrangements.

Here, the activity of the controller consists in the running of property dealing websites concerning properties in Hungary and written in Hungarian and thus pursues a real and effective activity in Hungary. Further, it has a representative in Hungary responsible for recovering the debts resulting from that activity and representing the controller in administrative and judicial proceedings relating to the processing of the data concerned. It has a bank account in Hungary intended for the recovery of debts and uses a letter box in Hungary for the management of everyday affairs. That is capable of establishing the existence of an “establishment”.

The processing is done in the context of the activities, which Weltimmo pursues in Hungary. Thus Hungarian data protection law would apply with respect to that processing. (By contrast the nationality of the persons concerned by such data processing is irrelevant.)

#### **6.4. INDEPENDENCE OF DPA**

Germany: Independence normally means a status, which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. There is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. The adjective "complete" implies a decision-making power independent of any direct or indirect external influence on the supervisory authority. The guarantee of independence of DPAs is intended to ensure the effectiveness and reliability of the supervision of compliance with data protection provisions, to strengthen the protection of individuals and bodies affected by their decisions. DPAs must act impartially and must remain free from any external influence, including that of the State or Lander. Independence precludes not only any influence exercised by supervised bodies, but also any directions or other external influence which could call into question the performance of those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.

State scrutiny in principle allows the government of the respective Land to influence the decision of the supervisory authority or cancel and replace those decisions. This is not consistent with the principle of independence.

Austria: By failing to take all measures necessary to ensure that the Austrian national legislation meets the requirement of independence with regard to the DSK, Austria has failed to fulfill its obligations under the second subparagraph of Article 28(1) of Directive 95/46 and Article 8(3) of the Charter of Fundamental Rights of the EU and Article 16(2) TFEU. The establishment in Member States of independent supervisory authorities is thus an essential component of the protection of individuals with regard to the processing of personal data.

The words “with complete independence” must be given an autonomous interpretation. Supervisory authorities must enjoy an independence which allows them to perform their duties free from external influence, direct or indirect, which is

liable to have an effect on their decisions. The fact that the DSK has functional independence insofar as its members are “independent and [are not] bound by instructions of any kind in the performance of their duties” is an essential, but not sufficient, condition to protect it from all external influence.

Here, the national legislation provides only for the operational autonomy of the supervisory authority, but does not preclude the DSK from performing its duties free from all indirect influence, for the following reasons:

The managing member of the DSK need not always be an official of the Federal Chancellery (although it always has been), and all day-to-day business is thus de facto managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision. It is conceivable that the evaluation of the managing member by his hierarchical superior for the purposes of encouraging his promotion could lead to a form of “prior compliance”. Moreover, the Chancellery is subject to the supervision of the DSK, so the DSK is not above all suspicion of partiality. The service-related link between the managing member of the DSK and the Chancellery affects the DSK's independence. The fact that the appointment of the managing member rests on an autonomous decision of the DSK does not protect the independence;

The office of the DSK is structurally integrated with the departments of the Federal Chancellery, and all DSK staff are under the authority of the Federal Chancellery and subject to its supervision. The DSK need not be given a separate budget to satisfy the criterion of independence. The DPA may come under a specified ministerial department. However, the attribution of the necessary equipment and staff to DPAs must not prevent them from acting with complete independence. Here, since they are subject to supervision by the Chancellery, it is not compatible with the requirement of independence.

The Federal Chancellor has the right to be informed of all aspects of the work of the DSK. This precludes the DSK from operating above all suspicion of partiality.

Hungary: Establishment in Member States of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data. Operational independence of supervisory authorities, in that members are not bound by instructions of any kind in the performance of their duties, is an essential condition that must be met to respect the independence requirement, but this is not sufficient. The mere risk that the state could exercise political influence over decisions of supervisory authorities is enough to hinder independence. If it were permissible for the Member State to compel the supervisory authority to vacate office before serving full term, even if this comes about as a result of restructuring or changing of the institutional model, the threat of such premature termination could lead the supervisory authority to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence, and the supervisory cannot be regarded as being able to operate above all suspicion of partiality. Member States are free to adopt or

amend the institutional model they consider most appropriate for supervisory authorities. However, they must ensure that the independence of the authority is not compromised, which entails the obligation to allow that authority to serve its full term.

Schrems: The Directive seeks to ensure an effective, complete, and high level of protection of the fundamental rights and freedoms of natural persons. The guarantee of the DPA's independence is intended to ensure effectiveness and reliability of the monitoring of compliance, and is an essential component of data protection.

## 6.5. DPA POWERS

Weltimmo: In the event that the Hungarian DPA should consider that Weltimmo has an establishment not in Hungary, but in another Member State, then in accordance with Article 28(4), it may exercise its powers conferred under Article 28(3) only within its own territory, and it may, irrespective of the applicable law and before even knowing which national law is applicable, thereby investigate the complaint. If it becomes apparent that it is the law of another Member State that applies, that DPA cannot impose penalties outside the territory of its own Member State. In fulfillment of the duty of cooperation laid down in Article 28(6), it requests the DPA of that Member State to establish an infringement of its national law and impose penalties if that law permits, based on the information which the first DPA has transmitted to second DPA. The second DPA may also find it necessary to carry out other investigations, on the instructions of the first DPA.

Schrems: DPAs powers extend to their own Member State, but not to processing in third countries. However, DPAs are responsible for monitoring transfers from a Member State to a third country, as the transfer is processing carried out in the Member State.

An adequacy decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46 is addressed to the Member States, which must take the necessary measures to comply with it. Until the Commission decision is declared invalid by the ECJ, it has legal effect in the Member States. However, the Commission decision cannot eliminate or reduce the powers of the DPA accorded by Article 8(3) of the CFR, and therefore cannot prevent data subjects whose personal data has been transferred from lodging a claim pursuant to Article 28(4) with the DPA alleging that an adequate level of protection is not ensured in that third country, which in essence challenges the validity of the Commission's adequacy decision. But the ECJ alone has jurisdiction to declare that the decision is invalid; neither the DPA nor a national court may do so. The latter must refer the claim to the ECJ for a preliminary ruling to examine the validity of the Commission decision.

Article 3 of Decision 2000/520 lays down specific rules regarding DPA's powers in light of a Commission adequacy finding (to suspend data flows to self-certified US organisations under restrictive conditions establishing a high threshold for intervention). It excludes the possibility of DPA's taking action to ensure compliance

with Article 25 (adequacy), in particular, it denies DPAs powers which they derive from Article 28 to consider a data subject's claim which puts into question whether a Commission adequacy decision is compatible with protection of privacy and fundamental rights and freedoms of individuals. This goes beyond the power conferred on the Commission in Article 25(6). Thus, Article 3 is invalid.

## **6.6. PROCESSING FOR SOLELY JOURNALISTIC PURPOSES**

*Tietosuojaaltuutettu*: Article 1 of the Directive indicates that the objective is that Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to processing of their personal data. That objective can only be pursued by reconciling those fundamental rights with the fundamental right to freedom of expression. Article 9's objective is to reconcile the two rights. Member States are required to provide derogations in relation to the protection of personal data, solely for journalistic purposes or artistic or literary expression, which fall within the fundamental right to freedom of expression, insofar as necessary for reconciliation of the two rights. To take account of the importance of the right of freedom of expression in every democratic society, it is necessary to interpret notions of freedom, such as journalism, broadly. Derogations must apply only insofar as strictly necessary. The fact that publication is done for profit making purposes does not preclude publication from being considered as "solely for journalistic purposes." The medium used is not determinative of whether it is "solely for journalistic purposes." Thus activities may be classified as "journalistic" if their sole object is the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit them.

## **6.7. PROCESSING FOR PURELY PERSONAL OR HOUSEHOLD ACTIVITY**

*Lindquist*: Mrs. Lindquist's activities were mainly charitable and religious, but these are not covered by the exceptions in Article 3(2) of the Directive and cannot be considered exclusively personal or domestic.

*Rynes*: Protection of the fundamental right to private life guaranteed under Article 7 of the CFR requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. Also, the wording of the derogation refers to "purely" personal or household activity, not simply a personal or household activity. Correspondence and the keeping of address books constitute, in the light of recital 12 to Directive 95/46, a purely personal or household activity, even if they incidentally concern the private life of other persons. However, to the extent that video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data, it cannot be regarded as a purely personal or household activity. In such case, the consent of the data subject would be required to process his data.

## 6.8. TRANSPOSITION/HARMONISATION

**Luxembourg:** A Member State may not plead provisions, practices or circumstances in its internal legal system (here, the new distribution of ministerial powers following a change in its internal government) in order to justify a failure to comply with obligations and time limits laid down in a Directive, and thus a violation had occurred relating to the transposition of Directive 95/46.

**Lindquist:** The Directive envisages complete harmonization, thus Member States must adopt national legislation conforming to the regime of the Directive. However, certain provisions of the Directive can explicitly authorize the Member States to adopt more constraining regimes of protection. This must be done in accordance with the objective of maintaining a balance between free movement of personal data and protection of private life. In addition, Member States remain free to regulate areas excluded from the scope of application of the Directive in their own way, provided no other provision of EU law precludes it.

**Promusicae:** Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in civil proceedings, nor does it oblige them to impose such an obligation. However, when transposing various intellectual property Directives, Member States must take care to interpret them such that there is a fair balance struck between the various fundamental rights protected by the Community legal order. Further, when implementing the national law transposing those Directives, authorities and courts of the Member States must interpret them in a manner consistent with the Directives and make sure that the interpretation does not conflict with those fundamental rights or other general principles of Community law, such as the proportionality principle.

**ASNEF:** Harmonisation of national laws is not limited to minimal harmonisation but harmonization, which is generally complete. Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of data subjects, equivalent in all Member States. Consequently, Article 7 of Directive 95/45 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as lawful. That interpretation is corroborated by the term “may be processed only if” which demonstrates the exhaustive and restrictive nature of the list appearing in that Article. Thus the Member States cannot add new principles relating to the lawfulness of processing or impose additional requirements.

Article 5 authorises Member States to specify the conditions under which the processing of personal data is lawful, within the limits of Article 7, *inter alia*. That margin of discretion can be used only in accordance with the objective pursued by the Directive of maintaining a balance between the free movement of personal data and the protection of private life. A distinction must be made between national measures that provide for additional requirements amending the scope of a principle



referred to in Article 7 (precluded) and national measures which provide for a mere clarification of one of those principles (allowed). Thus, Article 7(f) precludes any national rules, which in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions set out in that Article

Englebert: Article 13(1) states “Member States may” and thus does not oblige the Member States to lay down in their national law exceptions for the purposes listed therein. Rather they have the freedom to decide whether, and for what purposes, to take legislative measures aimed at limiting the extent of the obligations to inform the DS. Further, they may take such measures only when necessary.

## **6.9. DIRECT APPLICABILITY**

Rechnungshof: Wherever provisions of a directive appear to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any incompatible national provision, or insofar as they define rights which individuals are able to assert against the State.

ASNEF: Whenever the provisions of a Directive appear to be unconditional and sufficiently precise, they have direct effect if the Member State has failed to implement that Directive in domestic law by the end of the prescribed period. Article 7(f) is sufficiently precise, as it states an unconditional obligation.

## **7. DIRECTIVE 2002/58**

### **7.1. SCOPE**

Bonnier: The communication of name and address of a person using an IP address from which files were shared (for copyrighted audio books) falls within the scope of Directive 2002/58 (and within the scope of Directive 2004/48, dealing with copyright).

### **7.2. TRAFFIC DATA**

Probst: Article 6(2) of Directive 2002/58 provides an exception to the confidentiality of communications, stating that traffic data necessary for purposes of subscriber billing and interconnection payments may be processed “up to the end of the period during which the bill may lawfully be challenged or payment pursued”. Thus, the provision covers the processing necessary for securing payment, including debt collection.

Article 6(5) provides that traffic data processing authorized by Article 6(2) “must be restricted to persons acting *under the authority of* [service] providers of the public communications networks and publicly available electronic communications services

handling billing” and “must be restricted to what is necessary” for the purpose of such activity. Thus, the assignee of claims for payment is authorized to process the data on condition that it acts “under the authority” of the service provider and that it processes only traffic data which are necessary for the purpose of recovery of those claims. That provision seeks to ensure that such externalization of debt collection does not affect the level of protection of personal data enjoyed by the user. “Under the authority” must be strictly construed to mean that the assignee acts only on instructions and under the control of the service provider. The contract between the service provider and assignee must contain provisions ensuring the lawful processing of traffic data by the assignee and must allow the service provider to ensure at all times that those provisions are being complied with by the assignee.

## **8. DIRECTIVE 2006/24**

### **8.1. APPROPRIATE LEGAL BASIS**

Ireland: The Court rejected Ireland's argument that the sole or principal objective of the Directive 2006/24 is the investigation, detection and prosecution of crime. Article 95(1) provides that the Council is to adopt measures for approximation of provisions laid down by law, regulation or administrative action in the Member States which have the objective of establishment and functioning of the internal market. It may be used where disparities exist (or are likely to exist in the future) between national rules, which obstruct fundamental freedoms or create distortions of competition and thus have a direct effect on the functioning of the internal market. The premise of the Directive was to harmonize disparities between national provisions governing retention of data by service providers, particularly regarding the nature of data retained and periods of data retention. It was apparent that differences were liable to have a direct impact on the functioning of the internal market, which would become more serious with the passage of time.

Article 47 of the EU Treaty provides that none of the provisions of the EC Treaty may be affected by a provision of the EU Treaty, in order to safeguard the building of the *acquis communautaire*. Insofar as Directive 2006/24 comes within the scope of Community powers, it could not be based on a provision of the EU Treaty without infringing Article 47. Directive 2006/24 provisions are limited to activities of service providers and do not govern access to data or use thereof by police or judicial authorities of the Member States. They are designed to harmonize national laws on the obligation to retain data, the categories of data to be retained, the periods of retention of data, data protection and data security, and the conditions for data storage. They do not involve intervention by police or law enforcement authorities of Member States, nor access, use or exchange by them. Thus Directive 2006/24 relates predominantly to functioning of the internal market.

## 8.2. SCOPE

Bonnier: Directive 2006/24 deals exclusively with handling and retention of data generated by electronic communication service providers for the purpose of the investigation, detection, and prosecution of serious crime and their communication to competent national authorities. Thus a national provision transposing the EU intellectual property directive which permits an ISP in civil proceedings to be ordered to give a copyright holder information on the subscriber to whom the ISP provided an IP address allegedly used in an infringement is outside the scope of Directive 2006/24 and therefore not precluded by that Directive. It is irrelevant that the Member State concerned has not yet transposed Directive 2006/24.

## 8.3. LAWFULNESS

DRI: The material objective of Directive 2006/24 is of general interest – to ensure data are available for the purpose of the investigation, detection and prosecution of serious crime, and therefore to public security, and international terrorism. (Article 6 CFR lays down the right of any person to liberty and security.) Data relating to use of electronic communications are particularly important and a valuable tool in the prevention of offences and the fight against crime.

The proportionality principle requires that acts of EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation and do not exceed the limits of what is appropriate and necessary to achieve those objectives. Given the important role played by data protection in light of the fundamental right of privacy, and the extent and seriousness of the interference (of Directive 2006/24), the EU legislature's discretion is reduced, thus the review of that discretion should be strict. Retention of data is an appropriate tool for the objective pursued.

The fight against serious crime and terrorism is of utmost importance to ensure public security and its effectiveness may depend on the use of modern investigation techniques. But this does not, in itself, justify the retention measure being considered to be necessary. Derogations and limitations in relation to data protection must apply only insofar as strictly necessary. Here, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of the data. The need for safeguards is all the greater where personal data are subjected to automatic processing and there is significant risk of unlawful access to the data. Further, the Directive requires retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony – i.e. all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. It covers all subscribers and registered users – and therefore entails an interference with the fundamental rights of practically the entire European population. It does not mandate any link to crime.

Directive 2006/24 fails to lay down objective criteria by which to determine the limits of access of competent national authorities to the data and its use, nor substantive and procedural conditions relating to access by competent national authorities and to their subsequent use. It does not lay down objective criteria to limit the number of persons authorized to have access and use to what is strictly necessary, and is not made dependent on prior review carried out by a court or independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of obtaining the objective pursued.

The Directive establishes retention period of a minimum of 6 months and a maximum of 24 months, but it does not state that determination of the exact period must be based on objective criteria to ensure that it is limited to what is strictly necessary.

The Directive does not provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and unlawful access. It does not lay down rules adapted to the vast quantity of data whose retention is required, the sensitive nature of that data, and the risk of unlawful access, nor is there a specific obligation set on Member States to establish such rules. Rather, it permits providers to have regard to economic considerations when determining the level of security.

The Directive does not require that the data be retained within the EU, with the result that it cannot be held that the control by an independent authority of compliance with the requirements of data protection and security is fully guaranteed. This is an essential component of protection of individuals with regard to the processing of personal data.

Accordingly, the EU legislature exceeded limits imposed by compliance with principle of proportionality in light of Articles 7, 8 and 52(1) CFR.

## **9. ARTICLES 7, 8 CFR**

Schecke: The validity of legislation requiring publication must be assessed in light of provisions of the CFR, including Article 8. However, CFR Article 52(1) accepts that limitations may be imposed on rights under the CFR, as long as they are provided by law, respect the essence of those rights and are proportionate (necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Further, CFR Article 52(3) states that for rights in the CFR, which correspond to rights in the ECHR, the meaning and scope shall be the same as for the ECHR.

Publication must a) be provided by law, b) respect the essence of the rights and freedoms in CFR Arts. 7 and 8, and c) be proportionate (necessary and genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others). Here, publication is lawful since it is specifically provided for by the Regulation. It meets the general interest requirement because

publication is intended to enhance transparency regarding the use of CAP funds and sound financial management. Regarding proportionality, it is necessary to analyse whether the EU balanced its interest in guaranteeing transparency and ensuring best use of public funds with the rights of beneficiaries to privacy and data protection. Derogations to data protection are allowed only insofar as strictly necessary.

For natural persons, there is nothing to show that lawmakers made an effort to strike a balance. No automatic priority can be conferred on the objective of transparency over data protection, even if important economic interests are at stake. Thus, the lawmaker exceeded the limits, which the proportionality principle imposes.

Publication of the data in question with respect to the complainant legal person does not go beyond limits imposed by the proportionality principle. The seriousness of the breach manifests itself in different ways for legal persons versus natural persons. It would impose an unreasonable administrative burden on the competent national authorities if they were obliged to examine, before the data are published for each legal person who is a beneficiary, whether the name of that person identifies natural persons. Thus, the legislation requiring publication is valid with respect to the legal persons.

Schwartz: Taking and storing of fingerprints by national authorities, governed by Article 1(2) of Regulation 2252/2004, constitutes a threat to rights of respect for private life and protection of personal data.

Article 52(1) allows for limitations on exercise of rights in Arts. 7 & 8 as long as limitations are provided for by law, respect the essence of those rights, and respect proportionality (necessary and genuinely meet objectives of general interest recognised by EU or need to protect rights and freedoms of others). Here, the taking of fingerprints for passports is provided by Regulation 2252/2004 to prevent falsification of passports and prevent fraudulent use thereof, to prevent illegal entry into EU, therefore it pursues an objective of general interest recognised by the EU.

DRI: Directive 2006/24 does not permit retention of content, but it might have an effect on the use of the means of communication and consequently on the exercise of freedom of expression guaranteed by Article 11 CFR. It also directly affects private life (guaranteed by Article 7 CFR) and constitutes processing of personal data (and therefore falls under Article 8 CFR).

The obligation on providers of publicly available electronic communications services or public communications networks to retain data relating to a person's private life and his communications in itself constitutes an interference with Article 7. Access of competent national authorities to the data constitutes a further interference with that right. The Directive constitutes an interference with Article 8 because it provides for processing of personal data. The interferences with Articles 7 and 8 are wide-ranging and particularly serious. The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely

to generate in the minds of users the feeling that their private lives are the subject of constant surveillance.

Any limitation on the exercise of rights and freedoms laid down by the CFR must be provided by law, respect their essence and, subject to principle of proportionality, limitations may be made to those right and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. Even though retention constitutes a particularly serious interference with the right to privacy, it is not such as to adversely affect the essence of those rights given that the Directive does not permit the acquisition of knowledge of the content of the electronic communications. Nor does it adversely affect the essence of the right to protection of personal data because certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or public communications networks – to ensure appropriate technical and organizational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

Schecke: Publication on the website of data naming beneficiaries and amounts they receive constitutes interference with private life under CFR Article 7. It is irrelevant that data concerns activities of a professional nature, as under Article 8 ECHR, as the CFR has held that no principle justifies exclusion of activities of a professional nature from the notion of private life.

## **10. ARTICLE 8 ECHR**

Rechnungshof: The provisions of Directive 95/46, insofar as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in light of that right, which forms an integral part of the general principles of EU law. Article 8 ECHR states that public authorities must not interfere with the right to respect for private life, unless it is in accordance with law and is necessary in a democratic society to protect certain interests.

The collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8. The ECHR has held that communication of the data infringes the right of the persons concerned to respect for private life.

Regarding necessity, the purpose of the provision was to keep salaries within reasonable limits, which fits within the "economic well-being of the country". But "necessary" means that a pressing social need is involved and the measure is proportionate to the legitimate aim pursued. The authorities enjoy a margin of appreciation. The interests of the state must be balanced against the seriousness of the interference. The interference is justified only insofar as publication of the names is both necessary and appropriate to the aim of keeping salaries within reasonable

limits, which is for the national court to examine. If not, then the interference also constitutes a violation of Articles 6 and 7 of Directive 95/46.

V: Article 8 ECHR on private life relates to a fundamental right which covers the right to secrecy of one's medical state. The transfer of that data to a third party, even another EU institution, is an interference with that right, whatever the final use. Such interference may be justified if it is “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

Regulation 45/2001 establishes that inter-institutional transfers are foreseen. However, Article 7 is very general. Further, Article 6 states that personal data shall only be processed for purposes other than those for which they were collected if the change of purpose has been expressly foreseen by the rules of the EU institution, which was not the case here.

The criterion “necessary in a democratic society” is met if it is necessary to respond to a social imperative, and if it is proportionate to the legitimate end and the reasons specified are relevant and sufficient. The national authority has a limited margin of discretion. The right to privacy of medical data is protected by the EU juridical order, not only to protect the private life of the sick but also to preserve their confidence in the medical body and the medical services in general. The possibility to transfer such data to another institution calls for a particularly rigorous examination. Thus the interest of the Parliament to recruit a person able to exercise his duties must be balanced against the gravity of the interference of the right of the person concerned. The interest of the Parliament to conduct the medical examination does not justify the transfer without the consent of the person concerned. The data are very sensitive, were collected nearly two years before, for a specified purpose, by an institution for which the applicant did not work. The need of the Parliament could have been met by less intrusive means.

Article 1 specifies that EU institutions protect the fundamental rights of natural persons, in particular their right to privacy with respect to processing their personal data. Thus, the provisions of the Regulation may not be read as legitimising an interference to the right to privacy. The purpose for the Commission's collection of the data was to determine the applicant's fitness to perform the duties in the Commission's post. Using them to determine her fitness for the post with the Parliament constituted a change of purpose. Each institution is an independent employer, and is autonomous in the management of its personnel. The change of purpose was not foreseen in any legal text.

\* \* \*

## **APPENDIX 1: RECITALS [1 to 173]**

### **1. Data protection as a fundamental right**

The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

### **2. Respect of the fundamental rights and freedoms**

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

### **3. Directive 95/46/EC harmonization**

Directive 95/46/EC of the European Parliament and of the Council seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

### **4. Data protection in balance with other fundamental rights**

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

### **5. Cooperation between Member States to exchange personal data**

The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including



natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

## **6. Ensuring a high level of data protection despite the increased exchange of data**

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

## **7. The framework is based on control and certainty**

Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

## **8. Adoption into national law**

Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

## **9. Different standards of protection by the Directive 95/46/EC**

The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an

obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

## **10. Harmonised level of data protection despite national scope**

In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

## **11. Harmonisation of the powers and sanctions**

Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

## **12. Authorization of the European Parliament and the Council**

Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

### **13. Taking account of micro, small and medium-sized enterprises**

In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC

### **14. Not applicable to legal persons**

In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

### **15. Technology neutrality**

In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

## **16. Not applicable to activities regarding national and common security**

This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities, which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

## **17. Adaptation of Regulation (EC) No 45/2001**

Regulation (EC) No 45/2001 of the European Parliament and of the Council applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

## **18. Not applicable to personal or household activities**

This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors, which provide the means for processing personal data for such personal or household activities.

## **19. Not applicable to criminal prosecution**

The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council (7) Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

## **20. Respecting the independence of the judiciary**

While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

## **21. Liability rules of intermediary service providers shall remain unaffected**

This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

## **22. Processing by an establishment**

Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements.<sup>3</sup>The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

## **23. Applicable to processors not established in the Union if data subjects within the Union are targeted**

In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

## **24. Applicable to processors not established in the Union if data subjects within the Union are profiled**

The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

## **25. Applicable to processors due to international law**

Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

## **26. Not applicable to anonymous data**

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

## **27. Not applicable to data of deceased persons**

This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons

## **28. Introduction of pseudonymisation**

The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

## **29. Pseudonymisation at the same controller**

In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken

technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller

### **30. Online identifiers for profiling and identification**

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them

### **31. Not applicable to public authorities in connection with their official tasks**

Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

### **32. Conditions for consent**

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a



request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

### **33. Consent to certain areas of scientific research**

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

### **34. Genetic data**

Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained

### **35. Health data**

Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council<sup>1</sup> to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

### **36. Determination of the main establishment**

The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union

should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

### **37. Enterprise group**

A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

### **38. Special protection of children's personal data**

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counseling services offered directly to a child.

### **39. Principles of data processing**

Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

### **40. Lawfulness of data processing**

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

### **41. Legal basis or legislative measures**

Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice

to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

## **42 . Burden of proof and requirements for consent**

Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

## **43. Freely given consent**

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

## **44. Performance of a contract**

Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

## **45. Fulfillment of legal obligations**

Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does

not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

#### **46. Vital interests of the data subject**

The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

#### **47. Overriding legitimate interest**

The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and

fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest

#### **48. Overriding legitimate interest within group of undertakings**

Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

#### **49. Network and information security as overriding legitimate interest**

The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

#### **50. Further processing of personal data**

The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and

purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, *inter alia*: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

## **51. Protecting sensitive personal data**

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is

allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, *inter alia*, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

## **52. Exceptions to the prohibition on processing special categories of personal data**

Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

## **53. Processing of sensitive data in health and social sector**

Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on



Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

#### **54. Processing of sensitive data in public health sector**

The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (11), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

#### **55. Public interest in processing by official authorities for objectives of recognized religious communities**

Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

#### **56. Processing personal data on people's political opinions by parties**

Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

## **57. Additional data for identification purposes**

If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

## **58. The principle of transparency**

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

## **59. Procedures for the exercise of the rights of the data subjects**

Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

## **60. Information obligation**

The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to

ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

## **61. Time of information**

The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

## **62. Exceptions to the obligation to provide information**

However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

## **63. Right of access**

A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health,

for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

#### **64. Identity verification**

The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

#### **65. Right of rectification and erasure**

A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public

interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

## **66. Right to be forgotten**

To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

## **67. Restriction of processing**

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

## **68. Right of data portability**

To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or

maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

## **69. Right to object**

Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

## **70. Right to object to direct marketing**

Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

## **71. Profiling**

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal

effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

## **72. Guidance of the European Data Protection Board regarding profiling**

Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

## **73. Restrictions of rights and principles**

Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal

penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

#### **74. Responsibility and liability of the controller**

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

#### **75. Risks to the rights and freedoms of natural persons**

The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.



## **76. Risk assessment**

The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

## **77. Risk assessment guidelines**

Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

## **78. Appropriate technical and organisational measures**

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfill their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

## **79. Allocation of the responsibilities**

The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

## **80. Designation of a representative**

Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

## **81. The use of processors**

To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of

conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

## **82. Record of processing activities**

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

## **83. Security of processing**

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

## **84. Risk evaluation and impact assessment**

In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature,

particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

## **85. Notification obligation of breaches to the supervisory authority**

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

## **86. Notification of data subjects in case of data breaches**

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

**87. Promptness of reporting / notification**

It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

**88. Format and procedures of the notification**

In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

**89. Elimination of the general reporting requirement**

Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

**90. Data protection impact assessment**

In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged

for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

## **91. Necessity of a data protection impact assessment**

This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

## **92. Broader data protection impact assessment**

There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

## **93. Data protection impact assessment at authorities**

In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the

specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

#### **94. Consultation of the supervisory authority**

Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

#### **95. Support by the processor**

The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

#### **96. Consultation of the supervisory authority in the course of a legislative process**

A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

#### **97. Data protection officer**

Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist

of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

## **98. Preparation of codes of conduct by organisations and associations**

Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

## **99. Consultation of stakeholders and data subjects in the development of codes of conduct**

When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

## **100. Certification**

In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.



## **101. General principles for international data transfers**

Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

## **102. International agreements for an appropriate level of data protection**

This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

## **103. Appropriate level of data protection based on an adequacy decision**

The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

## **104. Criteria for an adequacy decision**

In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the

third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

#### **105. Consideration of international agreements for an adequacy decision**

Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

#### **106. Monitoring and periodic review of the level of data protection**

The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No

182/2011 of the European Parliament and of the Council (12) as established under this Regulation, to the European Parliament and to the Council.

### **107. Amendment, revocation and suspension of adequacy decisions**

The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

### **108. Appropriate safeguards**

In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

### **109. Standard data protection clauses**

The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent

controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

### **110. Binding corporate rules**

A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

### **111. Exceptions for certain cases of international transfers**

Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

### **112. Data transfers due to important reasons of public interest**

Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping

in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

### **113. Transfers qualified as not repetitive and that only concern a limited number of data subjects**

Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

### **114. Safeguarding of enforceability of rights and obligations in the absence of an adequacy decision**

In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

### **115. Rules in third countries contrary to the Regulation**

Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, *inter alia*, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

### **116. Cooperation among supervisory authorities**

When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

### **117. Establishment of supervisory authorities**

The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

**118. Monitoring of the supervisory authorities**

The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

**119. Organisation of several supervisory authorities of a Member State**

Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

**120. Features of supervisory authorities**

Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

**121. Independence of the supervisory authorities**

The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

## **122. Responsibility of the supervisory authorities**

Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

## **123. Cooperation of the supervisory authorities with each other and with the Commission**

The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

## **124. Lead authority regarding processing in several Member States**

Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially



affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

### **125. Competences of the lead authority**

The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

### **126. Joint decisions**

The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

### **127. Information of the supervisory authority regarding local processing**

Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of

which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

### **128. Responsibility regarding processing in the public interest**

The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

### **129. Tasks and powers of the supervisory authorities**

In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation.. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

### **130. Consideration of the authority with which the complaint has been lodged**

Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

### **131. Attempt of an amicable settlement**

Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

### **132. Awareness-raising activities and specific measures**

Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

### **133. Mutual assistance and provisional measures**

The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no

response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

#### **134. Participation in joint operations**

Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

#### **135. Consistency mechanism**

In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

#### **136. Binding decisions and opinions of the Board**

In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

#### **137. Provisional measures**

There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity, which should not exceed three months.

### **138. Urgency procedure**

The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

### **139. European Data Protection Board**

In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

### **140. Secretariat and staff of the Board**

The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

### **141. Right to lodge a complaint**

Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the

data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form, which can also be completed electronically, without excluding other means of communication.

#### **142. The right of data subjects to mandate a not-for-profit body, organisation or association**

Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

#### **143. Judicial remedies**

Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned, which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority, which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities, which are

not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them. Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State.

In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

#### **144. Related proceedings**

Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

#### **145. Choice of venue**

For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the

controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

#### **146. Indemnity**

The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

#### **147. Jurisdiction**

Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council should not prejudice the application of such specific rules.

#### **148. Penalties**

In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage



suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

#### **149. Penalties for infringements of national rules**

Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

#### **150. Administrative fines**

In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

### **151. Administrative fines in Denmark and Estonia**

The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

### **152. Power of sanction of the Member States**

Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system, which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

### **153. Processing of personal data solely for journalistic purposes or for the purposes of academic, artistic or literary expression**

Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

### **154. Principle of public access to official documents**

This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation.<sup>7</sup> In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the reuse of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

### **155. Processing in the employment context**

Member State law or collective agreements, including ‘works agreements’, may provide for specific rules on the processing of employees’ personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

### **156. Processing for archiving, scientific or historical research or statistical purposes**

The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to

appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfill those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

### **157. Information from registries and scientific research**

By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

### **158. Processing for archiving purposes**

Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should

not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

### **159. Processing for scientific research purposes**

Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

### **160. Processing for historical research purposes**

Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

### **161. Consenting to the participation in clinical trials**

For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply.

### **162. Processing for statistical purposes**

Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the

limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

### **163. Production of European and national statistics**

The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council provides further specifications on statistical confidentiality for European statistics.

### **164. Professional or other equivalent secrecy obligations**

As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

### **165. No prejudice of the status of churches and religious associations**

This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

### **166. Delegated acts of the Commission**

In order to fulfill the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms,

information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

### **167. Implementing powers of the Commission**

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

### **168. Implementing acts on standard contractual clauses**

The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

### **169. Immediately applicable implementing acts**

The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

### **170. Principle of subsidiarity and principle of proportionality**

Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the

principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

### **171. Repeal of Directive 95/46/EC and transitional provisions**

Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

### **172. Consultation of the European Data Protection Supervisor**

The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012.

### **173. Relationship to Directive 2002/58/EC**

This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council<sup>1</sup>, including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation.

\* \* \*



**APPENDIX 2: EU/ EEA NATIONAL SUPERVISORY AUTHORITIES**

<b>Sr. No</b>	<b>Country</b>	<b>National Data Protection Authority</b>	<b>Website</b>
1	United Kingdom	The Information Commissioner's Office	<a href="https://ico.org.uk">https://ico.org.uk</a>
2	Austria	Österreichische Datenschutzbehörde	<a href="http://www.dsb.gv.at">www.dsb.gv.at</a>
3	Belgium	Commission de la protection de la vie privée	<a href="http://www.privacycommission.be">www.privacycommission.be</a>
4	Bulgaria	Commission for Personal Data Protection	<a href="http://www.cpdb.bg">www.cpdb.bg</a>
5	Croatia	Croatian Personal Data Protection	<a href="http://www.azop.hr">www.azop.hr</a>
6	Cyprus	Commissioner for Personal Data Protection	<a href="http://www.dataprotection.gov.cy">www.dataprotection.gov.cy</a>
7	Czech Republic	The Officer for Personal Data Protection	<a href="http://www.uoou.cz">www.uoou.cz</a>
8	Denmark	Datatilsynet	<a href="http://www.datatilsynet.dk">www.datatilsynet.dk</a>
9	Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	<a href="http://www.aki.ee/en">www.aki.ee/en</a>
10	Finland	Office of the Data Protection Ombudsman	<a href="http://www.tietosuoja.fi/en">www.tietosuoja.fi/en</a>
11	France	Commission Nationale de l'Informatique et des Libertés - CNIL	<a href="http://www.cnil.fr">www.cnil.fr</a>
12	Germany	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	<a href="http://www.bfdi.bund.de">www.bfdi.bund.de</a>
13	Greece	Hellenic Data Protection Authority	<a href="http://www.dpa.gr">www.dpa.gr</a>
14	Hungary	Data Protection Commissioner of Hungary	<a href="http://www.naih.hu">www.naih.hu</a>
15	Iceland	Icelandic Data Protection Agency	<a href="http://personuvernd.is">http://personuvernd.is</a>
16	Ireland	Data Protection Commissioner	<a href="http://www.dataprotection.ie">http://www.dataprotection.ie</a>
17	Italy	Garante per la protezione dei dati personali	<a href="http://www.garanteprivacy.it">www.garanteprivacy.it</a>
18	Latvia	Data State Inspectorate	<a href="http://www.dvi.gov.lv">www.dvi.gov.lv</a>
19	Liechtenstein	Data Protection Office	<a href="http://www.dss.llv.li">www.dss.llv.li</a>
20	Lithuania	State Data Protection	<a href="http://www.ada.lt">www.ada.lt</a>
21	Luxembourg	Commission Nationale pour la Protection des Données	<a href="http://www.cnpd.lu">www.cnpd.lu</a>
22	Malta	Office of the Data Protection Commissioner	<a href="http://www.dataprotection.gov.mt">www.dataprotection.gov.mt</a>
23	Netherlands	Autoriteit Persoonsgegevens	<a href="https://autoriteitpersoons">https://autoriteitpersoons</a>

			gegevens.nl
24	Norway	Datatilsynet	www.datatilsynet.no
25	Poland	The Bureau of the Inspector General for the Protection of Personal Data – GIODO	www.giodo.gov.pl
26	Portugal	Comissão Nacional de Proteção de Dados - CNPD	www.cnpd.pt
27.	Romania	The National Supervisory Authority for Personal Data Processing	www.dataprotection.ro
28	Slovakia	Office for Personal Data Protection of the Slovak Republic	www.dataprotection.gov.sk
29	Slovenia	Information Commissioner	www.ip-rs.si
30	Spain	Agencia de Protección de Datos	www.agpd.es
31	Sweden	Datainspektionen	www.edoeb.admin.ch
32	Switzerland	Data Protection and Information Commissioner of Switzerland	www.edoeb.admin.ch
33	European Union	European Data Protection Supervisor	www.edps.europa.eu/EDPS WEB

## APPENDIX 3: LOOPHOLES IN GDPR

**The EU General Data Protection Regulation (GDPR) is an impressive act of legislation. Some people call it a great law.**

The GDPR sets out to provide individuals with protection of their personal data. Secondary goals are to balance the rights of individuals against other rights (including public interest) and to ensure a consistent rule of law for personal data throughout the EU. These goals had to be translated into words that can be legally enforced. The law has ended up with *a lot* of words—more than 55,000—the result of four years of negotiations between the many interested parties. Naturally, there are imperfections. Some businesses and others don't like the law and would prefer to avoid it when they can. They will be exploring the imperfections, looking for loopholes.

### FIVE LOOPHOLES—SUMMARY

#### 1. 'Controllers' outside the EU

The GDPR is meant to protect people in the EU when their personal data is controlled by organisations outside the EU, but it may not. Weaknesses in the wording of the law give the chance for organisations to collect data and ignore the GDPR. Once data 'escapes' from the GDPR, it can be passed on to others without legal protection. The GDPR states a couple of times in its recitals that protection of personal data of natural persons should take place "whatever their nationality or residence". The previous data protection directive covered any organisation processing personal data in the EU but did not guarantee the protection of every person in the EU (when their data was processed by an organisation outside the EU). The authors of the GDPR set out to change this, to cover any organisation in the EU that handles personal data and any individual in the EU whose personal data is handled by an organisation, wherever that organisation is based.

The reasoning is obvious. An individual can enter a website and give their personal data, without knowing where their data will be processed. The legislators wanted to give people the assurance that EU law would protect them in all cases.

Take the analogy of going to buy something at a shop in the EU. The purchaser is protected by EU consumer law and doesn't have to think twice about it—the shopkeeper cannot say "this product is from India and therefore we apply Indian laws of product safety and consumer rights". The GDPR has set out to create the same situation in the online world: you are protected, full stop.

The devil is in the detail, in the wording of the law. The GDPR states that its territorial scope includes the processing of personal data of someone in the EU by organisations outside, "where the processing activities are related to the offering of goods or services" to that person. The phrase "the offering of goods or services" is subject to different interpretations.

You could reasonably ask, why doesn't the regulation just say "related to the marketing or supply of goods or services" or perhaps even simpler "related to a data subject in the EU"? However, the GDPR was written by lawyers and this wording of "offering" originates from legalese applied in the context of EU competition law. There is ample case law regarding its interpretation, based on the definition of "undertaking" meaning an entity that carries on an "economic activity" and that the measure of an economic activity is "offering goods or services" (even if no payment occurs). The case law shows a broad interpretation of "offering goods or services" to cover sales, supply and even purchasing.

Therefore, the original drafters who decided to put in the words "offering goods or services" probably intended to cover any marketing or commercial activity that engages an individual in the EU (with the words "irrespective of whether a payment of the data subject is required" added later in the drafting process to ensure that it covers the new business models of online services such as social media).

Nevertheless, when the regulation was negotiated—and there was a lot of lobbying—words were added to a recital (the 'contextual' paragraphs before the main articles of the regulation) which took a different point of reference for interpreting "offering goods or services". Guided perhaps by the idea that an "offer" takes place before any transaction, the following words were added to Recital 23:

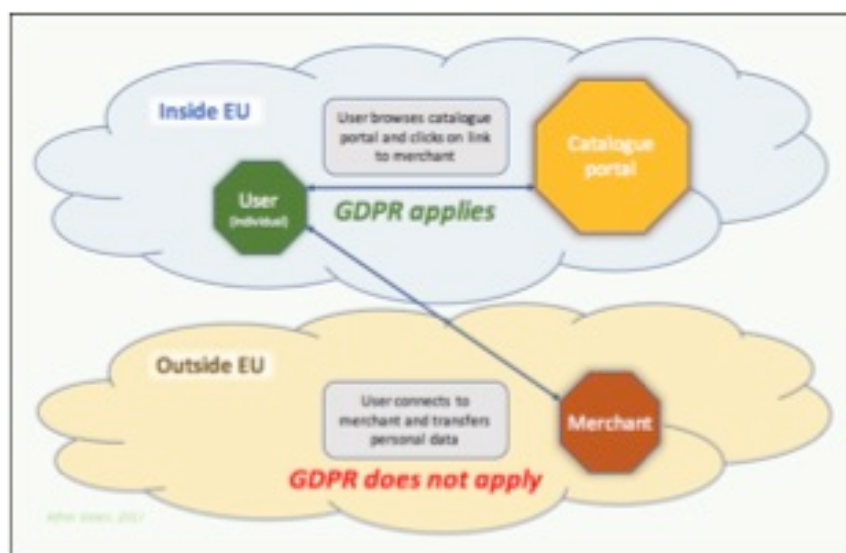
In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

This wording says that the test is based on whether the organisation "envisages" offering goods and services, not on whether it does in fact offer, or supply, or simply obtain personal data.

This wording originates from a legal judgment that determines in which jurisdiction within the EU (in other words, in which EU country) a case should be heard in a court of law. This case, combining two different actions known as *Pammer* and *Hotel Alpenhof*, was judged in 2010 by the CJEU and therefore forms part of EU case law. However, the nature and effect of this case is quite different from the context used in the GDPR. Firstly, the court was asked to determine in which jurisdiction a court case should be held, not to determine the territorial scope of application of a law. Secondly, the result was to make a defendant's claim subject to one of two

alternative member state courts, not **to either award or deny the protection of a law**. (Note: The GDPR contains explicit provisions for determining the jurisdiction, both for administrative and judicial processes.)

Untitled1.jpg We can imagine the scenario of, let's say, a Chinese company that markets a broad range of products and services that are sourced from third parties. This Chinese company creates a global portal, with a large catalogue of items. The catalogue is accessible worldwide, and might include European languages—and possibly a currency conversion tool to see prices in Euros—thereby presumably constituting an “offering” to people in the EU, but only in the sense of marketing, not selling products. Potential customers would browse this catalogue anonymously and, when they decide to buy a product or service, they click the appropriate link. This link would then take the individual to the website of an independent third-party company, outside the EU (whose website perhaps is not at all EU-centric, being written in English and Chinese, with prices in US dollars). The personal data interchange then takes place with this third-party company.



Following GDPR Recital 23 could put personal data outside the scope of the law

The original company with the catalogue portal would not handle any personal data, so it would not be subject to the GDPR. The third-party company would have deniability about offering goods or services to someone in the EU, since it

simply placed its products in a global catalogue. Any personal data given over would escape the scope of the GDPR.

Even without this slightly complicated scenario, there is a problem in the detail of the GDPR wording: “where the processing activities are related to the offering...” Effectively this does not cover any processing of personal data that arise from the “offering”, but only the processing activities related to the offering. If “offering” is interpreted narrowly, to only being the phase prior to a transaction or provision of a service, then all the processing activities that take place later—when the most personal data would be obtained—are not covered.

So, a global company wanting to find a loophole in the GDPR can set up a marketing company in the EU. Having done the minimal personal data processing needed to obtain customers, these customers are then transferred for transaction fulfillment, including personal data handling, to a non-EU business.

Once the personal data are “outside the law”, they stay outside the law—if not transferred back into the EU. A non-EU company with personal data, and not subject to any restrictions under the GDPR, could sell on the data to any other non-EU company.

The only evident way to block this loophole is for the CJEU to rule that Recital 23 is a misinterpretation of the purpose of the law and that “offering” should have the same interpretation as applied in competition law.

It should be noted that non-EU organisations might still become subject to the GDPR due to Article 3.2(b) that covers when processing activities are related to “the monitoring of their behaviour as far as their behaviour takes place within the Union”. This would cover tracking and profiling of individuals in the EU.

The proposed ePrivacy regulation, that is also due to come into force next year but is still at the drafting stage does not have this problem of territorial scope. The current draft covers “the provision of electronic communications services to end-users in the Union”, “the use of such services” and “the protection of information related to the terminal equipment of end-users located in the Union”. It does not have separate rules depending on the location of the provider (except that a non-EU provider has to designate a representative in the EU). It would cover, for example, any use of a website by a person who is in the EU (and any automated personal data collection, such as via cookies).

## **2. Data losing GDPR protection**

Even if data is collected and processed legally under the GDPR, it can be transferred to others and then escape the protection of the law. Personal data processed in the EU are clearly covered by the GDPR—no problems here. However, there are further consequences due to the way Article 3.2(a) describes the territorial scope.

Since, in the case of a non-EU data “controller” (an entity that processes data), it is only subject to the GDPR when *the processing activities are related to the offering of goods or services* to the individual in the EU (or monitoring the behaviour of the person), the same personal data could be processed for another purpose without being subject to the GDPR.

Take an example of a US-based company that collects personal data from someone in the EU. The company complies with the GDPR and follows a valid consent process to get the agreement from the data subject, saying “Please give your permission to process your data so that we can offer you a tailor-made service.” The individual gives their permission, the company carries out its processing accordingly.

Then the company sells the data to a third company, also in the US. This onward transfer of data would normally count as processing under the GDPR, but since this is a processing activity not related to the offering of goods or services to the individual, it is now outside the scope of the GDPR. Of course, the company buying the data is not subject to the GDPR since its processing of the data will also not be

related to an offering of goods or services (and certainly not to processing activities related to this).

The personal data will have leaked out of the GDPR scope. The only hope would be to try and ‘catch’ this data again, if and when it is used to direct an offering to someone in the EU. It could be very difficult to spot that this is happening via targeted advertising, and even harder to find the controller responsible.

It could be difficult to close this loophole. However an EU court would look to the purpose of an EU law when making a judgement and not just to specific wording of a provision, so it is perhaps feasible that the CJEU could determine that the words “related to” in the phrase “processing activities related to the offering of goods or services” should be interpreted to include “arising from” the processing activities—therefore saying that any personal data collected during the original processing activities would continue to enjoy the protection of the law when used for alternative purposes.

### **3. Invisible data chain**

If organisations obtain data indirectly, in most cases (and excluding loophole 2) it should still be subject to the GDPR. However, the application of the law in these cases may be only theoretical, particularly in the case of “data chains”. The intention of the GDPR is that individuals will always know what is happening with their data and will be able to exercise rights over this data. For example, data subjects have the right to access data held by a controller, correct errors, object to processing and request erasure. The starting point for exercising these rights is given in Article 15: “The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.”

However, how does the data subject know to which controller it has to ask this question?

Transparency is meant to start from the point of data collection. The controller has to provide a set of information to the data subject at this time, in accordance with Article 13. One of the items of information that the controller has to provide is “the recipients or categories of recipients of the personal data, if any”. A “recipient” is a third party to whom the controller discloses or transfers data.

The controller is not obliged to provide the names of recipients since it can choose to only provide the “categories of recipients”. Even if the individual does an access request, the controller can still limit the response to categories. Under Article 14 of the GDPR, each recipient controller would have to inform the data subject within a month of receiving the data. But what if the recipient doesn’t do this?

There might be valid reasons why the recipient controller does not provide this data. It might not be able to identify the data subjects whose data it has (and it has to have a high level of confidence that it doesn’t provide the data to the wrong person). Even if the individuals are identifiable, the recipient controller may not have their

contact details. Nothing in the GDPR obliges a controller to provide enough information to a recipient to allow it to comply with its (the recipient's) obligations under the GDPR and the controller itself is no longer legally liable (except in the case of joint controllers).

If an individual does discover that a company is using its personal data (for example, if they receive a direct marketing communication from a company they do not recognise), then the person can make an access request under Article 15. However, it might be impossible to find out from where that company got the data since the obligation on the company is only to provide “any available information about the source”. Furthermore, Recital 61 says “Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.”

The subject of non-identification of the individual concerned is covered by Article 11. A controller that cannot identify the data subject is absolved from having to respond in detail to a data subject's requests—except to tell the data subject (“if possible” to do so) that it cannot comply due to lack of identification. The individual can provide the controller with further information to aid the identification, but how this would work in practice is not clear. Although Article 11 does not exempt the controller from complying with Article 21, the right to object, nor to the provision of this article that requires a data subject to be informed of their right to object, at the latest at the time of the first communication, this right has no value if the controller never communicates directly.

Then, of course, there will be controllers that decide to ignore their obligations under the law. Unless they communicate directly with the individuals whose data they have, or do something flamboyant with the data that attracts attention, complaints are unlikely and their non-compliance may well go undetected.

In reality, there are currently long ‘data chains’, with personal data held several steps removed from the data subjects. Personal data is bought and sold like a commodity and whole industries, have developed on the back of this data interchange. Despite the clear obligations under the GDPR, these invisible data chains are likely to exist for a long time: perhaps few businesses in the chain will have the motivation or the means to comply and make Article 14 notifications. In many cases, the lawful basis for processing this data does not exist—or was based on pre-GDPR consent implementation—so businesses will not want to declare that they have the data.

In the best of scenarios, there will probably be a continuing black market for personal data.

Closing this loophole would require proactive steps by supervisory authorities to study data chains in operation and pinpoint businesses for enforcement action without waiting for complaints. Also, the modalities for informing data subjects under Article 14 could be facilitated: by encouraging controllers in direct contact with data subjects to be a conduit for Article 14 notifications from the recipients to



whom they provide data and introducing a special provision in the forthcoming ePrivacy regulation that explicitly recognises, subject to conditions, the use of unsolicited communications in order to comply with GDPR notification requirements.

#### **4. Inferred data**

Personal data is any data related to a living person. The GDPR gives obligations to processors of the data and it gives rights to individuals. But, even when the data stays personal, users may lose a number of rights. Organisations can take advantage of this. The term “inferred data” is not perfect—other phrases are sometimes used, such as “derived data”. It means data that is not in the original format that was collected, but which could still be considered personal data because it is related to an identifiable person.

Examples could range from simple categorisation (such as when a person says that they live in postcode 10963, Germany, and their file is automatically tagged with “Berlin”) to cases where there are human comments (such as when a doctor examines a patient and writes “symptoms of bronchitis” in the file). It could be a car navigation service that classifies a person as a “fast” driver, based on observed behaviour, in order to estimate driving times for that individual; it could be a tag to indicate that someone has a propensity to be susceptible to food-related advertising if presented before 9am.

This kind of data can in some cases fall under the definition of ‘profiling’, that is explicitly covered in the GDPR in the context of direct marketing or when automated decisions are made on the basis of profiling that have a legal or significant effect on the person. (Another little glitch in the GDPR is that a person can object to direct marketing based on profiling and have it stopped immediately, but there is no obligation on the controller to inform the data subject that any profiling is taking place—unless it produces “legal effects...or similarly significantly affects him or her”—despite a recital that does not include this limitation.)

A 2014 CJEU judgment (*YS v Minister voor Immigratie*) determined that a legal analysis of an individual is not “in itself” personal data, even though it contains personal data, and therefore the data subject was denied the right to get a copy of this analysis. This conclusion was on the basis that the analysis was an assessment of how an external factor (in this case, relevant laws) applied to the situation of the data subject, not information related to the data subject. A further reason was that an individual’s right of access to their personal data was in place to allow the person to verify the accuracy of the personal data and that it is processed in a lawful manner (and thereby exercise other rights, such as rectification or erasure), and access to the analysis was not necessary for this purpose.

This appears to conflict with the GDPR (a subsequent law), in which Recital 63 states that an individual should have the right to access their personal data, including “access to data concerning their health, for example the data in their

medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided”. An “assessment” by a physician would appear to fall into the same category as the “analysis” that was the subject of the 2014 legal case.

However, recitals only serve to convey the purpose and help to interpret the articles of an EU law—a recital cannot derogate from the actual provisions (articles) of the law. In Article 15.4 (covering a data subject’s access rights), the GDPR states “The right to obtain a copy [of the individual’s personal data] referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.” This is backed up by further words in Recital 63: “That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.”

The “others” here can be legal entities, such as the controller of the data. Any time a controller combines personal data from an individual with data from another source, or transforms it through an algorithm, they could use the reasoning from the 2014 “YS” judgment and refuse to provide a copy of this data.

Taking this a step further, an organisation wanting to keep personal data about individuals, without being subject to many of the obligations that come from GDPR rights for data subjects, could simply transform the data by some method (probably by a ‘proprietary’ algorithm, to increase the levels of legal defence). This method could even be reversible, allowing the organisation to re-create the original personal data if wished—in the meantime, deleting the individual’s original raw data on the principle of data minimisation.

The resulting data would still, probably, be legally recognised as containing personal data and so the organisation would need to observe the provisions of the GDPR: processing the data lawfully, only doing so for the defined purpose, minimising the data held, keeping it up-to-date, minimising the storage time, maintaining security of the data and being ready to be held accountable. However, it would only need to tell data subjects (in response to requests) about the categories of personal data held but not the details—and would not have to provide a copy (assuming the interpretation of the law given above).

If individuals cannot access a copy of the data, they will not know exactly what data is held. They will not be able to correct inaccuracies, nor of course contest the ‘inferences’ made by the data controller. Even if they had given consent to use of the original data, they would not be able to obtain data portability of the inferred data. They would be left with the right to withdraw consent, or to object to all data processing or to require erasure of all records, but this would be an “all or nothing” result that might not be practical for an individual—implying, for example, withdrawing entirely from a social media platform.

Closing this loophole probably requires further case law on the interpretation of “personal data”, particularly in the context of the GDPR rather than the 1995 data protection directive. Future case law on the meaning of “legal effects....or similarly

significantly affects”, in the context of profiling, would also be relevant due to the explicit rights given to individuals in this situation.

## 5. Legitimate interests

It may seem reasonable that organisations should be able to process personal data if they have a good reason to do so, after considering the interests of the individuals involved. However, the way this will work in practice means that many organisations could see it as a loophole in the law. The concept of “legitimate interests” of the organisation processing personal data has not changed from the 1995 data protection Directive, and the wording of the provision in the GDPR is almost identical. It requires that the controller balances its own (or a third party’s) legitimate interests against the interests or fundamental rights and freedoms of the data subject. Unless the data subject’s rights override the controller’s rights, it can proceed with the processing.

In the past, most businesses did not elect to use “legitimate interests” as the lawful ground for using personal data because it does require an assessment of the balance of interests and this could be subject to later challenge. In most EU jurisdictions, there has been a lax regime applied to the use of ‘consent’ from individuals—with it normally being sufficient to give a data subject an opt-out option covering a broad usage of the personal data—so businesses having tended to go this route. Once they had a ‘consent’, they didn’t need to provide any further justification for what they were doing.

This is changing. The GDPR definition of consent is more demanding than that of the 1995 directive and—crucially—the GDPR is a regulation that automatically applies across the EU. The 1995 directive had to be transposed into national legislation, which gave a lot of scope for different interpretation in different countries. Some national legislation did not even include the definition of data subject consent that was specified in the directive.

In addition, the supervisory authorities that ensure organisations comply with data protection law have indicated that they are going to take a strict approach to judging whether consents have been obtained validly. From May 2018, all consents must be according to GDPR definitions. Since this means specific ‘opt-in’ consents, businesses can assume that they will receive far fewer consents than under the old regime. Organisations handling personal data, particularly those that are in the business of marketing, are in general revising their data protection procedures to use the claim of legitimate interests instead of consent.

Processing personal data on the basis of legitimate interests should not be a loophole. It has been long accepted as valid, since there are many situations where individuals would accept the processing of their personal data and may not want to be bothered by the mechanisms of giving consent. They have not lost their rights in this case. They can still request access to their data, object to processing and pursue other rights such as rectification and erasure.

However, the problem is in the procedure.

Data controllers, that might be commercial businesses, should have a good idea of their own legitimate interests—to make money can be one of them. They have to balance their own well-defined legitimate interests against the diffuse and varied interests of the mass of the data subjects, probably applying a single approach for all potential subjects. As was indicated by the Article 29 Working Party, in its opinion on legitimate interests, the interests of the data subjects are highly dependent on context and may depend on the personal circumstances of the person.

Under the GDPR—except in cases where there is a high risk to individuals, such as in large-scale processing of sensitive data—the data controllers independently make their assessment of the balance of interests, without supervision and without consulting with the data subjects themselves. The controller has to inform the individual (under Article 13) that it is using a legitimate interests ground for the processing, and it has to describe its own (or a third party's) legitimate interests, but it does not have to say what interests of the data subject it has taken into account, nor how it has calculated the balance of interests.

If the individual makes a 'subject access request', for details of the personal data processing that are taking place, at this point the controller does not even have to tell the person that the processing depends on a legitimate interests assertion. (It is presumably assumed that the data subject was notified at the time of data collection.)

The recourse is meant to be via the right to object, according to Article 21. This is the only way a data subject can find out how a data controller decided that its own legitimate interests were of greater value than his or her own interests. The wording of Article 21.1 is:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(Note that it is presumed that the objection is expected to be on the basis of the "particular situation" of that individual, implying that any assessment of the balance of interests will only be applicable to that one person.)

The problem with this stage of the procedure is that the assertion of predominant legitimate interests by a controller against a whole body of data subjects is then only questioned in the circumstances of individual cases.

Furthermore, when the controller is called upon to "demonstrate" its compelling legitimate grounds that override the interests of the individual, there is no process defined for a potential independent assessment. Presumably the controller has to

demonstrate its position to the data subject, but there is no requirement to inform the supervisory authority or anyone else—unless the data subject is unhappy and complains.

Nearly all organisations, particularly those with commercial interests, will take a decision on how to deal with the GDPR in terms of a balance of cost, risk and reward. This will not be the “risk” as generally covered by the GDPR, which is the risk to the rights and freedoms of individuals through misuse of their personal data, this will be the risk to the enterprise.

The costs, risks and rewards equation of using ‘consent’ looks bad (for commercial organisations with traditional business models) under the GDPR:

- **Costs:** Structuring and implementing a good consent procedure could be expensive.
- **Risks:** If any single consent is ruled invalid, this would probably apply to all consents under the same procedure and so processing of all the data subjects involved would have to stop immediately.
- **Rewards:** Since the procedure is ‘opt-in’ there will be a much lower take up by data subjects compared to ‘opt-out’.

The costs, risks and rewards equation of using ‘legitimate interests’ looks good, even if the balance of interests calculation is done unfairly biased towards the interests of the organisation:

- **Costs:** These may not be so high, since it is an internal exercise and the level of effort put into the balance of interests calculation can be kept low if there is little risk of having to justify it.
- **Risks:** Falling foul of the law is unlikely, since the methodology of the balance of interests calculation will probably never be tested. In response to any individual complaint, the controller can just accept the objection of that person and stop processing their data, so not having to justify the original logic and continuing to process the data of others without change. If there were so many complaints that it were to come to attention of the supervising authority, the organisation can simply defend itself on the basis of the many ‘judgmental’ calls that had to be made when calculating the balance of interests. If the organisation can show basic diligence by reference to an impact analysis conducted at the start, a significant fine is extremely unlikely.
- **Rewards:** Since this effectively turns ‘legitimate interests’ processing into an opt-out procedure, the organisation will be able to process the data of nearly all the people it wants, just reducing the numbers to the degree that it receives objections/opt-outs.

This loophole arises from the impossibility of defining precise rules to conduct a balance of interests assessment, combined with a procedure that theoretically puts the burden of proof on the controller but in practice leaves controllers almost

unsupervised. The loophole does not apply in the case of processing sensitive data, since a controller's legitimate interest is not a lawful basis to do this (excluding the special cases of healthcare and certain non-profit bodies). However, most processing of personal data does not include sensitive data.

One solution will be if there is a shift back towards the use of 'consent', but under the GDPR rules. For some businesses, this might occur due to the forthcoming e-Privacy regulation, see Consent: lost and found. Another would be a more generalised use of 'contract'.

It appears that responsibility for minimising the effect of this loophole will fall to supervisory authorities. However, these authorities will be overwhelmed with more definitive responsibilities once the GDPR is applied and, in absence of public complaints, their duty to act on legitimate interest issues is somewhat nebulous. Probably the best that can be hoped is that opinions from the European Data Protection Board (that replaces the Article 29 Working Party next year), guideline documents from the supervisory authorities and codes of conduct from industry bodies (Article 40) will draw clear lines about how to apply the balance of interest calculations and reduce the margin of tolerance for controllers that rely on dubious legitimate interests claims.

## **Conclusions**

This article has focused on five significant loopholes in the GDPR. Another article will describe weaknesses of the regulation that might undermine its success even without any conscious abuse.

However, this article comes with a health warning: it has not attempted to make a balanced judgment of the GDPR. Despite any imperfections, the GDPR is already having a major effect on all industries that make use of personal data—in nearly all cases giving more protection and more usable rights to individuals. Keeping the loopholes as small as possible will have a big impact on its overall success.

\* \* \*

## APPENDIX 4: FLOW CHART – COMPOSITION OF EUROPEAN DATA PROTECTION BOARD

